
Combating Terrorism

# 2005 TSWG REVIEW

## Technical Support Working Group

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **2005** | **N/A** | **-** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **2005 TSWG Review, Combating Terrorism** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Technical Support Working Group (TSWG) Washington, DC 20402-0001** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release, distribution unlimited**

13. SUPPLEMENTARY NOTES
**The original document contains color images.**

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **SAR** | **96** | |

**Standard Form 298 (Rev. 8-98)**
Prescribed by ANSI Std Z39-18

# Preface

*Wars are not won without sacrifice -- and this war will require more sacrifice, more time, and more resolve. The terrorists are as brutal an enemy as we have ever faced -- unconstrained by any notion of common humanity or by the rules of warfare. No one should underestimate the difficulties ahead -- nor should they overlook the advantages we bring to this fight.*

*President George W. Bush*
*October 28, 2005*

Terror has been an enduring tactic employed by our enemies throughout the history of the United States. In this modern era, we face a rapidly evolving global battlefield and a transformative enemy that embraces terrorism in new ways, thus posing new challenges. The recent attacks in Amman, London, Bali, New Delhi, and Baghdad tragically illustrate the shifting terrain as the United States and our international partners confront an unrelenting non-state enemy that seeks, with random murder and destruction, to terrorize individuals, nations, and the civilized world.

***"Revolutionary advances in technology are transforming war in our favor."***

***George W. Bush***
***May 27, 2005***

*Perhaps the greatest impetus for modernization and cooperation is the specter of lethal threats confronting all free nations.*

*Secretary of Defense Donald H. Rumsfeld*
*June 4, 2005*

Our enemy is evil, but he is not senseless. Terrorists are remarkably adept at discerning our strengths and weaknesses and improvising ways to succeed. Our foes exploit the explosive growth of media and the Internet, as well as the ease of travel and communication around the world. These technical advances have made possible the proliferation of new tactics and capabilities that we must counter as we confront our enemies. We must be more agile than the terrorists and use our resources well to counter them and prevent the carnage and political upheaval that they seek to inflict.

In the war on terror, the United States employs a variety of instruments of statecraft to meet its objectives. These techniques include diplomacy, intelligence collection and analysis, enhanced security measures, financial controls, law enforcement activities, and military action. The Technical Support Working Group (TSWG) is an additional instrument that cuts across a number of these areas: TSWG develops and uses science and technology to thwart or to respond to terrorist attacks and to support and enhance the capabilities of the other instruments of statecraft.

# Preface

Since 1986, TSWG has developed and transitioned technologies for combating terrorism in the broad context of national security by providing a cohesive and inclusive forum to define and fulfill user-based technical requirements spanning the Federal interagency community. By harnessing the creative spirit of U.S. and foreign industry, academic institutions, and government and private laboratories, TSWG (through the activities of its functional subgroups) nurtures a robust community for defining, agreeing to, and cooperatively developing technical solutions to the most pressing counterterrorism needs. This cooperative, interagency focus fosters a consensus-based approach to the rapid prototyping and development of combating terrorism devices, training tools, reference materials, software, and other equipment that has wide utility in the counterterrorism community at large.

***"To meet the threats of the 21st century, we are developing new technologies that will make our forces faster, lighter, more agile, and more lethal."***

***George W. Bush***
***May 27, 2005***

*Defeating a broad and adaptive network requires patience and constant pressure and strong partners in Europe, in the Middle East, and North Africa, and Asia and beyond. Working with these partners, we are disrupting militant conspiracies, destroying their ability to make war, and are working to give millions in a troubled region of the world a hopeful alternative to resentment and violence.*

*President George W. Bush*
*October 28, 2005*

In addition to the primary focus on serving the needs of Federal Government end users, TSWG has demonstrated for over a decade that international cooperation is an enduring element in the successful development of technologies for combating terrorism. Our international partners have experience confronting terrorists that comes only from time, they share our beliefs and ideals, they are technologically proficient, and they are situated in key locations around the globe. The United States works to ensure that nations willing to fight terrorism have the means to do so, and TSWG is an important part of that process.

In this report, you will read about a selection of new technical capabilities developed by TSWG over the past twelve months, in addition to selected examples of combating terrorism technologies and capabilities that are currently under development. This report is representative and not exhaustive in its presentation of TSWG projects, capabilities, and technologies.

# Preface

The nation and the world should recognize that we are making steady progress in the fight against terrorism on a variety of fronts. TSWG and its national and international programs are among the essential advantages that we bring to this fight.

*We will all stand until terrorism is defeated and until those who simply want to live a normal life and to live in peace can return to the days when this sort of tragedy, this sort of outrage, does not happen.*

*Secretary of State Condoleezza Rice*
*November 14, 2005*

# Table of Contents

# The Technical Support Working Group (TSWG)

# The Technical Support Working Group

## History and Mission

In April 1982, National Security Decision Directive 30 assigned responsibility for the development of overall U.S. policy on terrorism to the Interdepartmental Group on Terrorism (IG/T), chaired by the Department of State (DOS). TSWG was an original subgroup of the IG/T, which later became the Interagency Working Group on Counterterrorism (IWG/CT). In its February 1986 report, a cabinet-level Task Force on Counterterrorism, led by then Vice-President Bush, cited TSWG as assuring "the development of appropriate counterterrorism technological efforts."

Today, TSWG still performs that counterterrorism technology development function as a stand-alone interagency working group. TSWG's mission is to conduct the national interagency research and development (R&D) program for combating terrorism requirements. It also has commenced efforts to conduct and influence longer-term R&D initiatives and, reflecting the shift to a more offensive strategy, balance its technology and capability development efforts among the four pillars of combating terrorism: antiterrorism, counterterrorism, intelligence support, and consequence management.

## Organization and Structure

TSWG operates under the policy oversight of the Department of State's Coordinator for Counterterrorism and the management and technical oversight of the Department of Defense (DoD) Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD(SO/LIC)). While TSWG's core funds are derived principally from DoD's Combating Terrorism Technology Support (CTTS) Program and DOS, other departments and agencies contribute additional funds and provide personnel to act as project managers and technical advisors.

TSWG has successfully transitioned capabilities to the Departments of Agriculture, Defense, Justice, State, and Treasury; the Intelligence Community; the Transportation Security Administration; the Public Health Service; and many other departments and agencies. Additionally, TSWG has transitioned many systems to State and local law enforcement.

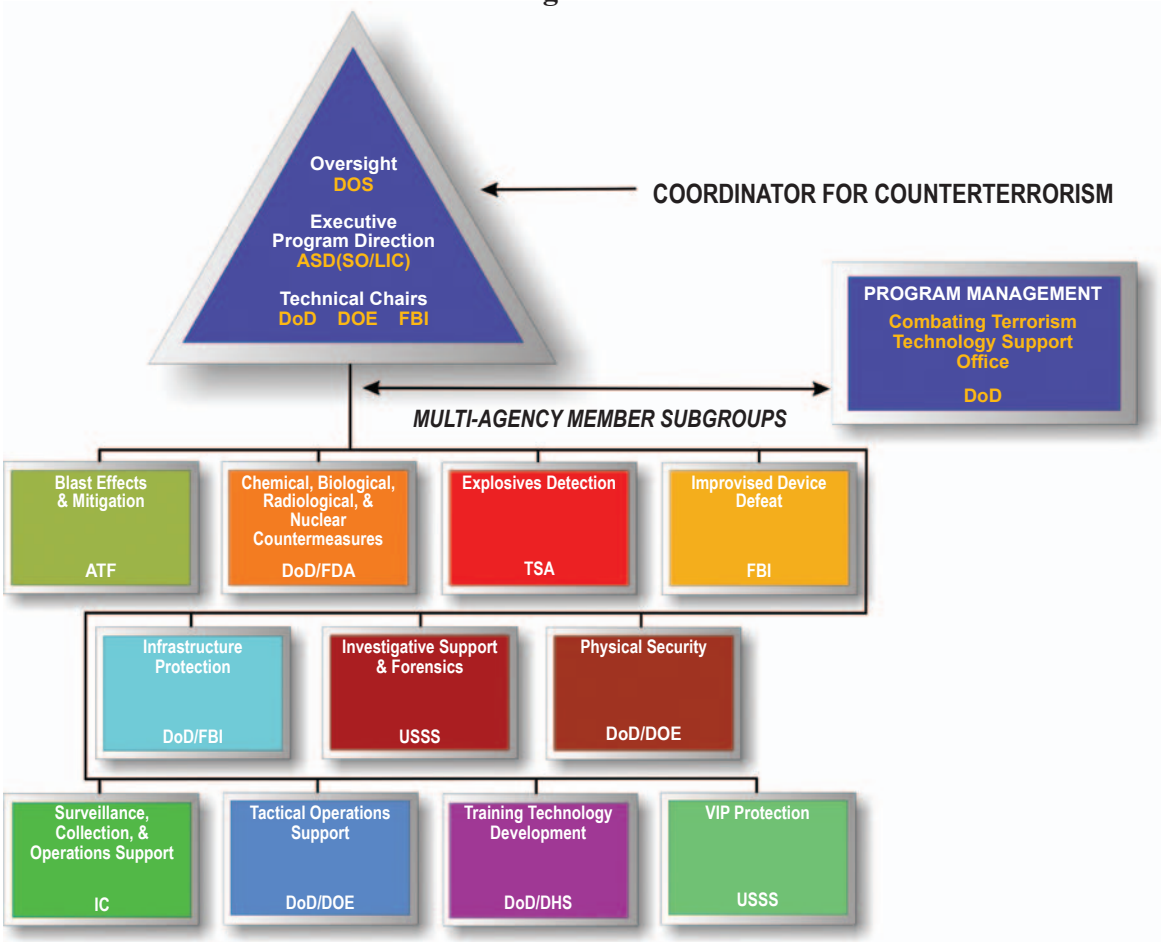
TSWG membership includes representatives from over 100 organizations across the Federal Government. These departments and agencies work together by participating in one or more subgroups. Participation traditionally has been open to Federal departments and agencies, but with the increasing importance of first responders, appropriate representatives from State, local, and international agencies are invited to participate on an as-needed basis. A comprehensive listing of member organizations by subgroup is provided in the appendix.

# The Technical Support Working Group

The eleven TSWG subgroups are:

- Blast Effects and Mitigation;
- Chemical, Biological, Radiological, and Nuclear Countermeasures;
- Explosives Detection;
- Improvised Device Defeat;
- Infrastructure Protection;
- Investigative Support and Forensics;
- Physical Security;
- Surveillance, Collection, and Operations Support;
- Tactical Operations Support;
- Training Technology Development; and
- VIP Protection.

**TSWG Organization**




Each subgroup is chaired by a senior representative from a Federal agency with special expertise in that functional area. Chairmanship of five subgroups is shared as indicated in the organizational chart above.

# The Technical Support Working Group

## International Program

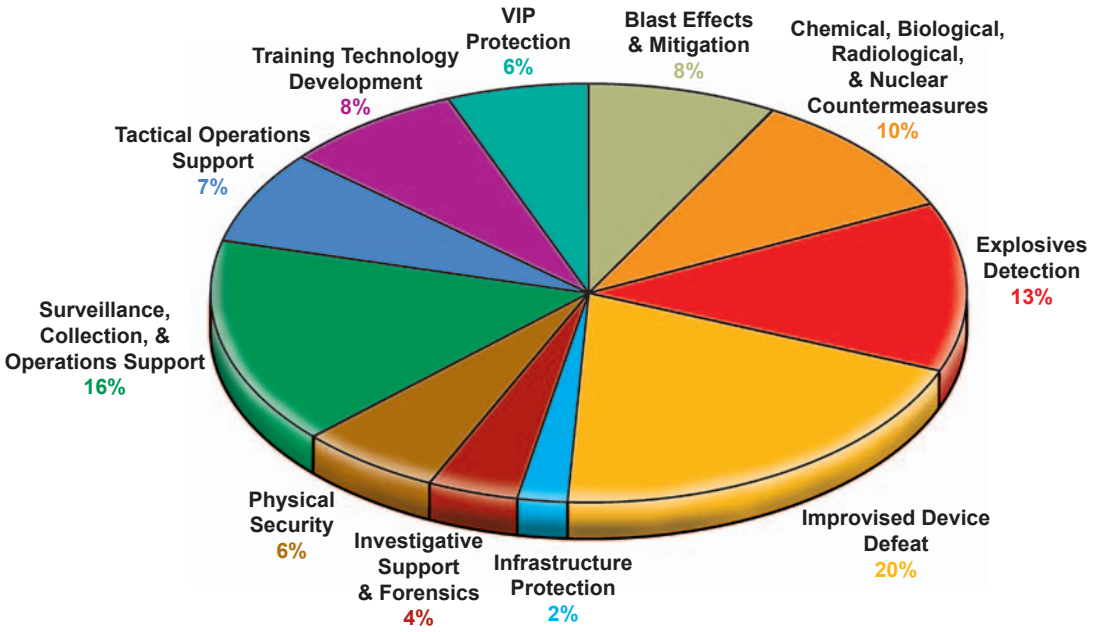
As demonstrated by recent events in London, Bali, and Amman, the terrorist threat is indeed global in nature. To be effective, the response must be global and coordinated as well.

In 1993, the U.S. Congress—recognizing the international nature of the terrorist threat in that era—authorized TSWG in the DoD budget appropriation process to conduct collaborative research and development in the area of combating terrorism with select NATO and major non-NATO allies. Cooperative agreements were subsequently concluded with Israel, the United Kingdom, and Canada. Recently, two additional agreements (with Australia and Singapore) have been negotiated and are awaiting authority to implement. Such international cooperation allows TSWG to leverage foreign experience, expertise, and resources in the Global War on Terrorism.

## Program Funding

Funding for the TSWG program has increased from over $11 million in FY 1995 to almost $203 million in FY 2005. This increase reflects the heightened concern over terrorist activity and the recognized need to accelerate the development of technology to effectively address the threat. The Department of Defense provides the bulk of funding for TSWG activities. The Department of State contributes annually to TSWG core funding, while other departments and agencies share the costs of selected projects.

**TSWG FY 2005 Program Funding ($202.8 Million)**



# The Technical Support Working Group Subgroups

Photo by USMC Sgt. T. L. Carter-Valrie

# Blast Effects & Mitigation

# Blast Effects and Mitigation

## MEMBERSHIP

**New York City Mass Transit Authority**

**Port Authority of New York/New Jersey**

**U.S. Department of Defense**
DTRA, USA (ARL, CE-PDC, SCC, USAISR), USAF (AFRL), USN (NAVFAC, NHRC)

**U.S. Department of Justice**
ATF

**U.S. Department of State**
DS

## Mission

***Identify, prioritize, and execute research and development projects that satisfy interagency and international requirements to define and mitigate the potential damage mechanisms from conventional and enhanced explosive mixtures.***

The Blast Effects and Mitigation (BX) subgroup identifies and develops technologies and techniques to evaluate the conventional and enhanced explosive effects on representative targets, including structures, critical infrastructure, vehicles, and humans. Projects conducted through this group characterize and provide interagency coordination of near-term solutions for emerging explosive threats. A representative from the U.S. Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives chairs the Subgroup.

## Focus Areas

The BX subgroup focus areas reflect the prioritized requirements of Federal engineering activities responsible for high risk facilities, the owners of critical infrastructure, and the needs of military personnel exploring new concepts in body armor and ballistic protection. During FY 2005, these focus areas were:

### Conventional and Enhanced Novel Explosive Mitigation

Investigate and characterize both conventional and novel explosives to fully understand the potential damage and to identify mitigation strategies. Emphasize the development, design, and construction of retrofit techniques for new and existing buildings, field fortifications, vehicles, and barriers in order to strengthen these structures and to reduce debris hazards and structural collapse.

### Advanced Instrumentation

Develop new, repeatable, and sustainable test protocols, instrumentation suites, and models that capture and characterize the dynamic environment of emerging threats. Use data and information obtained through comprehensive instrumentation test efforts to develop new protection and mitigation methodologies to specifically address enhanced novel explosives.

### Human Lethality in a Blast Environment

Quantify the effects of conventional and enhanced blast damage mechanisms to the human body. Evaluate the effectiveness of blast prevention and mitigation concepts from an injury perspective. Develop new methodologies to protect against blast fragmentation, fire, and overpressure injury.

# Blast Effects and Mitigation

### Critical Infrastructure Security

Test and evaluate critical structural systems in buildings, bridges, tunnels, and other critical infrastructure components using both full-scale blast testing and blast simulator technologies. Assess the level of protection that is sufficient to mitigate various threats to enable military planners and stakeholders in critical transportation systems to make more informed decisions.

### Information Products

Coordinate the exchange of test data, published reports, manuals, and guidance on blast mitigation. Produce blast and structural response guidance for conventional and enhanced novel explosives. Develop, design, and produce construction and retrofit techniques for new and existing structures, vehicles, and barriers.

## Selected Completed Projects

### Explosive Loading Laboratory Testing

Obtaining quality data from blast tests typically requires expensive live field tests. The University of California at San Diego (UCSD) developed a laboratory-based explosive loading simulator that allows blast effects research to take place with less live-explosive testing, resulting in significant cost savings. The Blast Simulator performs fully repeatable, controlled blast load simulations on critical structural elements (e.g., columns, beams, girders, walls, and floors) and on potentially lethal non-structural elements such as glass windows, masonry walls, and curtain walls. UCSD now uses the simulator to generate quality data for computer model validations for verification in a parametric investigation of blast retrofit designs, including the use of fiber-reinforced polymer composites, and for optimization of hardening technologies. Comparisons with field explosive testing validate the blast simulator data. Additional information on the simulator is available at http://www.jacobsschool.ucsd.edu/Englekirk.

### Curtain Wall Tests

Government and private-sector buildings in urban areas often use curtain walls to increase the level of blast protection of the building and its occupants. TSWG conducted a blast test to evaluate the response of a unique curtain wall system designed for the Federal Office Building Project. The blast test subjected a representative portion of the curtain wall system to the design threat. The test results allowed engineers to identify specific improvements to the design of the curtain wall. Requests for additional information should be sent to bxsubgroup@tswg.gov.

# Blast Effects and Mitigation

### COTS Testing

The Energetic Materials Research and Testing Center (EMRTC) employed COTS blast mitigation products and systems under the guidance of the various suppliers to conduct blast tests that accurately portray probable threats. EMRTC used dual electronic recording systems along with associated triggering systems that provided redundancy to ensure recovery of data. The products were tested for the effects of pressure, acceleration, force, strain, displacement, temperature, and other blast effects. The Center thoroughly evaluated all test data to draw conclusions on the blast mitigation effectiveness of specific COTS products and systems. Requests for additional information should be sent to bxsubgroup@tswg.gov.

### Suspender Rope Tests

Within the last year, TSWG completed a series of blast tests on components of suspension bridges at the request of several owners of such bridges. These tests were successful and yielded information about potential mitigation strategies. The results allowed the owners to make decisions on retrofit solutions. Requests for additional information should be sent to bxsubgroup@tswg.gov.

## Selected Current Projects

### Bridge Tower Testing

The protection of bridges is vital to maintaining the flow of commerce throughout the nation. This task focuses on determining the effects of blast and/or fire on key bridge types (truss, suspension, and post-tensioned) and the collapse mechanism of the failure. TSWG is evaluating the effects of a near-contact charge on various types of towers in order to determine the effects of explosions occurring near a bridge. The data from the live testing will validate existing computer models with various stand-off distances at roadway level as well as with bridge towers at waterways. Testing will also take into consideration construction materials and the age of the structure. The results of these tests will assist in the selection of mitigation techniques for critical pathway and iconic bridge types.

### Tunnel Retrofits

Determining the capacity of existing tunnels to withstand the gas pressure effects of explosive charges is essential to understanding and improving tunnel safety. To assess the need for tunnel retrofits, EMRTC is validating existing computer programs that are used to determine damage mechanisms. Areas of concern include the effect of soil interaction on the tunnel caused by the applied blast load, crack propagation caused by outside soil and/or water pressure, the blast effect on an adjacent tunnel, and the rate of water flow through the tunnel based on a breach scenario. Testing will occur in both steel and concrete tunnel structures.

# Blast Effects and Mitigation

### Blast Wall Tests

Building architects and planners in both the public and private sectors need the latest research and data available on the protective properties of construction material. TSWG is investigating methods for making walls more blast resistant. This effort includes testing new construction materials as well as testing both new and existing retrofit solutions, such as polymer application. The test results will be made available on a restricted basis to government and private-industry planners to facilitate their design and decision-making processes for new structures.

### Urban Environment Tests

The effects of large-scale detonations in an urban environment are not fully known. TSWG and a foreign partner are performing half-scale urban environment testing that will provide detailed information on the effects of a blast on the immediate and adjacent buildings. Current computer models will also be updated and validated with the live test data. Mitigation strategies will be tested and recommended based on the results of the tests.


### Waterside Protection

TSWG and a foreign partner are investigating underwater and surface blast impacts by small-boat improvised explosive devices to ships and waterside structures to determine survivability and recommend mitigation strategies. The research team is developing force protection concepts to better protect personnel, ships, and piers.

### Contact Information

bxsubgroup@tswg.gov

# Chemical, Biological, Radiological, and Nuclear Countermeasures

# Chemical, Biological, Radiological, & Nuclear Countermeasures

## MEMBERSHIP

ENVIRONMENTAL PROTECTION AGENCY

FEDERAL RESERVE BOARD

INTELLIGENCE COMMUNITY

INTERAGENCY BOARD

NEW YORK CITY FIRE DEPARTMENT

NEW YORK CITY POLICE DEPARTMENT

NUCLEAR REGULATORY COMMISSION

U.S. CAPITOL POLICE

U.S. DEPARTMENT OF AGRICULTURE
APHIS, ARS, FSIS

U.S. DEPARTMENT OF COMMERCE
NIST

U.S. DEPARTMENT OF DEFENSE
DATSD (CBD), DIA, DTRA, JCS, NSA, PFPA, USA (22ND CML BN(TE), 52ND ORD, CMLS, MANSCEN, NGIC, RDECOM-ECBC), USAF (ACC), USMC (CBIRF), USN (BUMED, NAVCENT, NAWC, NSWC)

U.S. DEPARTMENT OF ENERGY
SO

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
CDC, FDA, NIOSH

U.S. DEPARTMENT OF HOMELAND SECURITY
FEMA, ICE (FPS), S&T (HSARPA), TSA, USCG, USSS

U.S. DEPARTMENT OF JUSTICE
FBI, NIJ, USMS

U.S. DEPARTMENT OF STATE
DS, OBO, S/CT

U.S. POSTAL INSPECTION SERVICE

U.S. SENATE SERGEANT AT ARMS

## Mission

***Identify, prioritize, and execute interagency chemical, biological, radiological, and nuclear combating terrorism requirements and deliver technology solutions for detection, protection, decontamination, mitigation, containment, and disposal.***

The Chemical, Biological, Radiological, and Nuclear Countermeasures (CBRNC) subgroup identifies, validates, and prioritizes multi-agency user requirements and competitively seeks technological solutions for countering the terrorist employment of CBRN materials. Through its participation in the InterAgency Board for Equipment Standardization and InterOperability and in coordination with DHS, NIJ, and EPA, the CBRNC subgroup integrates technology requirements from the fire, hazardous materials, law enforcement, and emergency medical services communities into its process. Senior representatives from DoD and FDA co-chair the Subgroup.

## Focus Areas

The CBRNC subgroup focus areas reflect the prioritized requirements of the CBRN incident prevention and response community. During FY 2005, these focus areas were:

### Detection

Improve the sampling, detection, and forensic analysis of chemical, biological, and radiological threat agents in the air, in food or water, and on surfaces.

### Protection

Improve the operating performance and reduce the costs of individual and collective protection. Develop and enhance personal protective equipment, including respiratory protection systems and suits. Develop analysis and design tools for CBRN protection for building engineers and architects. Develop and evaluate advanced filter materials.

### Decontamination

Improve technologies and protocols for personnel, facilities, and equipment decontamination. Develop and enhance safe, low-cost, and environmentally benign systems to effectively decontaminate CB warfare agents and persistent toxic industrial chemicals and to mitigate a release of radioactive materials.

### Information Resources

Develop shared information management tools to provide a common "picture of the scene". Facilitate the efficient integration of diverse emergency and consequence management elements from Federal, State, and local agencies.

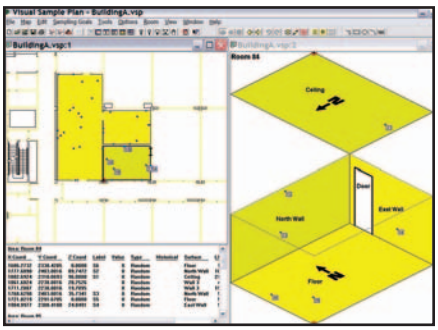
# Chemical, Biological, Radiological, & Nuclear Countermeasures

## Selected Completed Projects

### Distributed Chemical Sensor


The first Distributed Chemical Agent Sensing and Transmission (DiCAST®) system was installed at a regional airport facility in June 2005. This initial DiCAST® installation is providing a continuous line of protection in key segments of the facility against a high-priority military chemical agent and a toxic industrial chemical. DiCAST® integrates stable and sensitive reagents for rapid chemical detection within the plastic cladding of specially designed and drawn optical fibers. The sensing fibers respond to the presence of a toxic chemical in seconds, at concentrations less than 10% of the most common acute health effects regulatory limit. Requests for additional information should be sent to business@intopsys.com.

### Statistical Tool for Sampling Contaminated Buildings



The success of building decontamination following a CB event requires a statistically valid surface sampling plan to determine the extent of contamination. To guide the sample collection and decontamination process, Pacific Northwest National Laboratory (PNNL) developed a software tool to efficiently and effectively focus the efforts of decontamination personnel. PNNL enhanced the capabilities of an existing software package, the Visual Sample Plan (VSP). The enhanced VSP advises consequence management and emergency responders on how to best assess the contamination and to evaluate decontamination efforts. Version 4.0 of VSP was deployed in July 2005 and is freely available for download from the PNNL Web site at http://dqo.pnl.gov/index.htm.

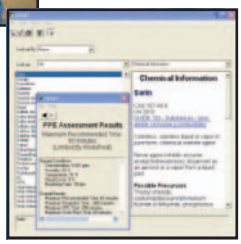
### Expedient Mitigation of a Radiological Release


To mitigate the effects of terrorist use of a radiological dispersion device, rapid containment of radioactive material is essential. First responders need materials, equipment, and procedures to quickly and efficiently remove radioactive surface contaminants. Isotron Corporation developed a novel coating technology and process for immediate countermeasures that support crisis response following an accidental or intentional radiological release. The technology provides a critical capability to first responders to prevent the unwanted spread of radionuclides and to facilitate subsequent restoration and decontamination efforts. In addition, two formulations of the coating, IsoFIX™ and HeloTRON™, were successfully field-tested as dust palliatives to mitigate the dangers associated with helicopter landings in desert conditions. Additional product details and contact information is available at the Isotron Web site at http://www.isotron.net/products.

# Chemical, Biological, Radiological, and Nuclear Countermeasures

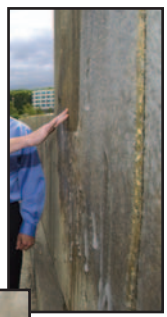

## Concentration and Extraction Techniques for Air Samples

High-volume air samplers are currently the most effective method to collect and concentrate air samples for chemical and biological agent detection at very low concentrations. Midwest Research Institute developed an ultra high-volume concentrating air sampler that uses an electrostatic precipitator with recirculating fluids and a proprietary vapor adsorbent. The system is capable of operating at 10,000 L/min while efficiently collecting chemical agents, agent precursors and degradation products, toxic industrial chemicals, and biological agents. The samples are delivered in matrices that are compatible with existing, validated analytical systems. Requests for additional information should be sent to cbrncsubgroup@tswg.gov.



## Chemical Risk Assessment Tool

There is no single standard personal protective equipment (PPE) ensemble for use by first responders when entering hazardous environments contaminated with chemical agents. Organizations maintain different inventories of chemical protective clothing and respirators suitable to individual budgetary and operational requirements. In parallel efforts, Georgia Tech Research Institute and AristaTek developed mobile emergency response tools that provide first responders with decision support for working in environments contaminated with chemical agents. These systems allow incident commanders to evaluate and select the best available PPE ensemble given the chemical agent, concentration, and ambient conditions faced. Incident commanders will be able to make rapid, accurate decisions regarding isolation, protective action distances, and hot-zone stay times. The software incorporates initial symptoms of exposure, odor thresholds, PPE breakthrough times, and exposure guidelines. Requests for additional information should be sent to cbrncsubgroup@tswg.gov.



## Radiological Decontamination Technologies for Post-Event Restoration

Removing subsurface soluble radionuclides following their intentional release into the environment is a challenge, especially for buildings and monuments where damaging the contaminated surface is not an option. The Argonne National Laboratory decontamination system operates much like an automated car wash; remote sprayers apply a wash agent and an adhesive superabsorbent gel. The gel draws the water from the pores of the building, carrying with it the radioactivity. Specially designed nanoparticles in the gel target the radioactive elements and bind them in the gel. The gel is then wet-vacuumed from the surface, leaving only a very small amount of radioactive waste for disposal. The Argonne technique overcomes many shortcomings of current radioactive decontamination operations, which are destructive to the surface and were not designed for use outside, in open environments. The prototype uses off-the-shelf spray-on technology and vacuum removal. Additional information is available at http://www.cmt.anl.gov/science-technology/processchem/supergel.shtml.

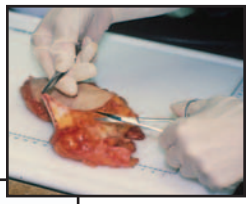
# Chemical, Biological, Radiological, and Nuclear Countermeasures

## Selected Current Projects

### Next-Generation Fire Fighter Protective Ensemble

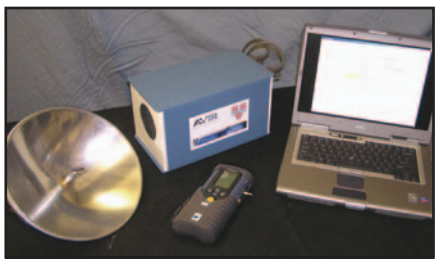
In responding to an event, fire fighters may have little or no indication of the involvement of CBRN hazards on-scene. Two parallel project teams, led by the International Association of Fire Fighters and North Carolina State University, are each designing protective clothing for structural fire fighting (i.e., bunker gear) to protect against CBRN challenges in addition to fire and heat. The project teams of first responders, material designers, and clothing-design experts are rapidly developing, testing, and prototyping personal protective equipment (PPE) system designs so that interface areas also provide effective protection, while adding CBRN protective qualities and improving thermal protection, comfort, and functionality. The bunker gear will be certified under the National Fire Protection Association (NFPA) 1971 optional CBRN standard. Following the completion of agent testing and expanded field evaluation programs, the prototype suits will be available in 2006.

### Low-Cost Personal Decontamination System




From either calculated terrorist acts or accidental releases, first responders face a wide range of chemical threats, including chemical warfare agents and toxic industrial chemicals (TICs). Addressing an unspecified threat requires a flexible and broad-spectrum decontamination system. Currently available systems have several drawbacks, including health hazards of corrosive detoxification agents, protocols requiring multiple preparation and execution steps, inability to collect all decontaminated materials, and limited shelf life. Moreover, there is a compounding hurdle of how to effectively treat eyes, mucous membranes, and wounds exposed to chemical agents. Starting with Reactive Skin Decontamination Lotion™, originally developed by Defence Research and Development Canada, Lawrence Livermore National Laboratory is developing a prototype personal decontamination system that will quickly remove or neutralize fast-acting military chemical agents and persistent TICs, including thickened agents, mustard, and chemicals that are sparingly soluble in water. The system will have a greater capacity and will be more compact than existing kits.

### Advanced Hybrid Chemical Detection System



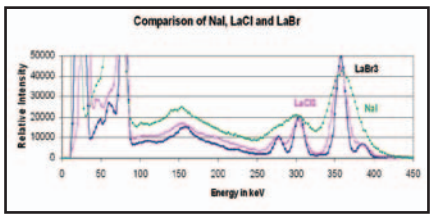
Existing sensor systems to detect chemical agents are either very expensive or provide limited sensitivity and response. Avir, LLC designed and built a hybrid detection system for building ventilation protection that combines an optical sensor (the TOVA™, a totally optical vapor analyzer designed by Avir) and a COTS point sensor. This unique detection system, which uses two methods to detect chemical warfare agents and toxic industrial chemicals (TICs), provides improved reliability, response time, and accuracy. The system is low-cost, robust, sensitive to a large number of chemicals, and can be trained to detect new chemicals. Existing detectors or combinations thereof currently cannot provide the advantages of

# Chemical, Biological, Radiological, and Nuclear Countermeasures

the TOVA™ hybrid system at an equally low cost. The system has undergone live-agent testing and environmental testing. Extended field-testing in select buildings is planned to begin in late 2005.

### Best Practices Handbook for Carcass Disposal

The potential for a catastrophic loss of livestock, poultry, or crops caused by disease, natural disasters, or deliberate acts of bioterrorism creates an urgent need for effective, efficient, and timely disposal of immense quantities of contaminated animal carcasses and plant material. The Texas Agricultural Experiment Station is developing a clear, concise, and easy-to-use handbook that will enable leaders to identify disposal methods that meet their needs for safe, fast, low-cost, and high-throughput disposal of contaminated plant and animal material with minimal environmental impact. The handbook will provide guidance based on engineering, economic, and regulatory analyses of options, building on experience and lessons-learned from responses to foreign and domestic natural outbreaks.

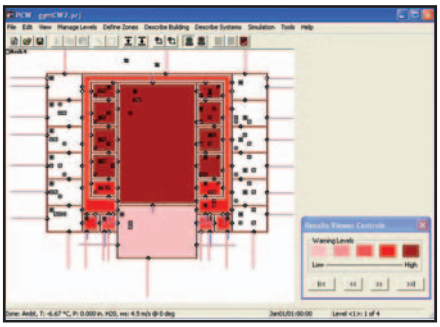



### Real-Time Radioisotope Identification and Reporting

Timely and accurate reporting of the time, place, nature, and severity of a radiological threat is essential to ensure the proper emergency response. The Advanced Radioisotope Identification System (ARIS) integrates a new room-temperature lanthanum bromide scintillation crystal with twice the resolution of the material in commonly used isotope identifiers. Better resolution will result in faster and more confident isotope identification. Each gamma-ray spectrum is tagged with Global Positioning System coordinates from the receiver built into the handset and sent via a wireless link to the base station, which can be located up to 200 yards away. The incident commander can then e-mail the spectrum from the remote incident location to Federal, State, or local command centers or technical analysis support cells over existing telecommunications paths. SAIC is designing and testing ARIS to meet the Performance Criteria for Hand-held Instruments for the Detection and Identification of Radionuclides standard (ANSI N42-34) adopted by DHS.

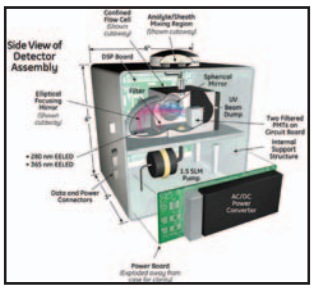
# Chemical, Biological, Radiological, and Nuclear Countermeasures

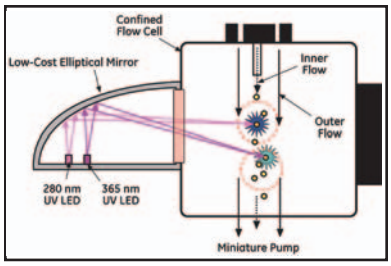
### Rapid Air Flow and Contaminant Transport Modeling



To determine contingency plans in the event of a terrorist attack or accidental agent release, building managers and engineers need to accurately and rapidly determine air flow rates and residence times for a facility. The Pennsylvania State University (Penn State) is developing CONTAM PCW, a software tool that will identify a set of simple measurements to confirm airflow predictions, which can then be used to refine the building model, guide security procedures, position sensors, and develop hazard response practices. The software is based on version 2.1 of CONTAMW, NIST's airflow and contaminant transport analysis software tool (publicly available on the Web). CONTAMPCW provides model tuning techniques and an enhanced, easier-to-use interface. Penn State is conducting large-scale building air flow tests to validate the model in late 2005.

### Biological Aerosol Threat Warning Detector




In the event of a biological attack, networked building sensors that alert building occupants to the presence of biological warfare agents could significantly decrease casualties. The system must be fast, accurate, and inexpensive; the goal is a "smoke detector" for biological aerosols. This project breaks new ground in materials science and optical design to bridge the gap between current capabilities and what is needed to inform building occupants of a potential threat. The system will act as a catalyst to initiate evacuation or protective action. Leading-edge semiconductor design is being used to optimize the output, reliability, and stability of ultraviolet light-emitting diode excitation sources for biological aerosol fluorescence. GE Global Research is developing a rapid, reliable sensor that indicates the presence of elevated airborne concentrations of microbiological material in air. The sensor triggers an alarm to permit space isolation and evacuation of building occupants.

## Contact Information

cbrncsubgroup@tswg.gov

# Explosives Detection

# Explosives Detection

## MEMBERSHIP

**U.S. Department of Defense**
DIA, NSA, USAF (AFESC, AFRL), USN (NAVEOTECHDIV, NRL)

**U.S. Department of Energy**
SO

**U.S. Department of Homeland Security**
ICE (FPS), S&T (HSARPA), TSA (FAMS), USCG, USSS

**U.S. Department of State**
DS

**U.S. Postal Inspection Service**

## Mission

***Identify, prioritize, and execute research and development projects that satisfy interagency requirements for existing and emerging technologies in the area of explosives detection and diagnostics. Emphasis is placed on a long-term, sustained approach leading to new and enhanced technologies for detection and identification of improvised explosive devices and large vehicle bombs.***

The Explosives Detection (ED) subgroup identifies and develops technologies to enhance the operational capability of both military and civilian applications. A representative from the Transportation Security Administration chairs the Subgroup.

## Focus Areas

The ED subgroup focus areas reflect the prioritized requirements of a broad range of interagency customers, including those responsible for physical security and forensic analysis. During FY 2005, these focus areas were:

### Vehicle-Borne IED Detection

Develop technologies necessary to provide a stand-off detection capability for explosives in large volumes at a distance. Investigate unique physical and chemical phenomena that identify the presence of explosives, the physical limits for sensor technology to respond to these phenomena, and enhancements to detection technology. Develop techniques to improve both stand-off distance and the types of explosives that can be detected. Evaluate remote techniques, in which a system is downfield from the operator but near the objects of interest, to afford a nearer-term solution. Explore longer-term technologies leading to a true stand-off detection capability.

### Suicide Bomber Detection

Improve systems that detect the presence of improvised explosive devices concealed by persons engaged in suicide attacks against government installations and public facilities, both domestic and international. Programs in this area are highly sensitive; specific capabilities generally cannot be discussed in an unclassified document.

### Short-Range Detection

Develop new explosive detection capabilities and improvements to existing systems for detection and diagnosis of concealed terrorist devices. Emphasize technologies that support entry-point screening. Improve detection rate, throughput, and accuracy in identification of explosives, as well as safety for both operators and the general public.

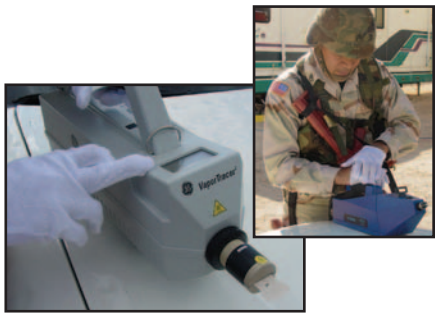
# Explosives Detection

### Canines

Develop training tools, protocols, and technologies that support and enhance canine detection of explosives. Improve canine team effectiveness and consistency through better understanding of both canine detection ability and of canine/human interaction.

## Completed Projects

### Handheld Explosive Detector Evaluation



TSWG assessed commercial handheld detectors for trace explosives as a way to screen for vehicle-borne improvised explosive devices. The results of this evaluation show that with proper tactics, techniques, and procedures, operators can use these detectors to find explosive residues on vehicles and other surfaces. The particle detection methods recommended by the manufacturers were generally effective. However, successful use of these detectors depends on the scenario in which they are used. Requests from government agencies for this report should be sent to edsubgroup@tswg.gov.

### Fluorescent Polymers for Explosives Detection

Sandia National Laboratories coordinated a multi-partner program to increase capabilities for polymer-based explosives detection. The Massachusetts Institute of Technology (MIT), in cooperation with Nomadics, Inc., developed a new fluorescent polymer for the detection of dimethyl dinitrobutane (DMNB), a marking agent for explosives. MIT is currently developing polymer compounds for potential use in the direct detection of royal demolition explosive (RDX) and peroxides, such as triacetone triperoxide (TATP). The follow-on efforts, including completion of the RDX and TATP polymers, are being funded through the Transportation Security Laboratory and the Air Force Research Laboratory. These polymers will be compatible with the Nomadics FIDO® explosives detection technology. Requests for additional information on these detection polymers should be sent to Nomadics at contacts@nomadics.com.

### Protective Boots for Deployed Military Working Dogs

Canine vehicle screening operations in desert environments are limited by extreme ground temperatures, which can average 120 to 140°F during the day. Canine handlers have resorted to pouring water on the ground to cool it off long enough for the canines to search vehicles at a checkpoint. To prolong the working time of the dogs on hot ground, TSWG purchased and evaluated canine boots for use in a screening operation. Initial feedback from the handlers is that the boots extend the working time of the canines. The boots also provide protection for the canines in environments where they could step on shattered glass and other debris. Individual dogs preferred different styles of boots. Additional information can be obtained from Thera-Paw, Inc. at http://www.therapaw.net, and Ruff Wear, Inc. at http://www.ruffwear.com.

# Explosives Detection

### Evaluation and Optimization of Explosives Trace Detection Portals

TSWG participated in a Transportation Security Administration (TSA) study to evaluate and optimize the performance of two explosives trace detection systems, the Smiths Detection Ionscan® Sentinel II and the GE EntryScan$^3$. The TSWG-funded efforts modified these systems to increase detection speed, to detect additional types of explosives, and to improve operational reliability. As a result of this study, TSA has purchased 44 trace detection portals from the two companies. Additional information on the GE EntryScan$^3$ portal is available at http://www.geindustrial.com/ge-interlogix/iontrack/prod_entryscan.html. Additional information on the Smiths Detection Ionscan® Sentinel II is available at http://194.105.117.18/products/Default.asp?Product=24.

## Current Projects


### Pressure-Activated Surface Sampler for Benchtop Trace Explosives Detectors

CyTerra Corporation is developing an automated device to facilitate benchtop trace explosives detection. The wand sampler rotates the sample collection wipe and standardizes the time and pressure used to remove material from surfaces. This step reduces the variability inherent in manual sample collection. When sampling is completed, the sampling wipe is inserted into the detector for analysis. Testing indicates that sampling performance is consistently equal to the best manual sampling technique.

### Combined X-Ray and Quadrupole Resonance Detection for Parcels and Hand Baggage

Rapiscan Systems has designed and built a prototype system for the inspection of hand-carried baggage that integrates quadrupole resonance capability for the detection of explosives with an existing airport X-ray system. The Rapiscan QXR-1000 system is similar in size to current airport baggage screening equipment. The prototype was delivered for Government evaluation in October 2005. Requests for additional information should be sent to edsubgroup@tswg.gov.

### Associated Particle Imaging for Vehicle-Borne IED Detection

Dynamics Technology, Inc. is developing a prototype system to detect bulk quantities of explosives inside closed cars and small to medium-sized trucks. This neutron-based technology is designed to locate explosives inside a vehicle by identifying the elements present in the vehicle and its contents, providing a clear indicator about the vehicle. This prototype is currently being designed for domestic checkpoint applications.

# Explosives Detection

**Detection of Hazardous and Explosive Liquids in Sealed Bottles and Cans**

Screening of sealed bottles and cans for hazardous or explosive liquids is required in certain security applications. Rapiscan Systems Neutronics and Advanced Technologies (formerly Ancore Corporation) is building a prototype system based on thermal neutron analysis for the non-invasive detection of hazardous and explosive materials in containers. The system will undergo testing in the second quarter of FY 2006.

## Contact Information

edsubgroup@tswg.gov

# Improvised Device Defeat

U.S. Department of Defense

# Improvised Device Defeat

## MEMBERSHIP

Fairfax County (VA) Police Department

Intelligence Community

National Bomb Squad Commanders Advisory Board

U.S. Capitol Police

U.S. Department of Defense
USA (52nd Ord, EOD Tech Det), USAF (ACC, EOD Det 63), USMC (CBIRF, MCD NAVEOTECHDIV), USN (NAVEODFLTLAU, NAVEOTECHDIV)

U.S. Department of Homeland Security
OUS-P, S&T (HSARPA), TSA, USSS

U.S. Department of Justice
ATF, FBI, NIJ, USMS

## Mission

***Identify, prioritize, and execute research and development projects that satisfy interagency requirements to more safely and effectively render terrorist devices safe. Particular emphasis is placed on technologies to access, diagnose, and defeat terrorist improvised explosive devices (IEDs); improvised chemical, biological, radiological, and nuclear (CBRN) devices; and vehicle-borne improvised explosive devices (VBIEDs).***

The Improvised Device Defeat (IDD) subgroup delivers advanced technologies, tools, and information to increase the operational capabilities of the U.S. military explosive ordnance disposal (EOD) community and Federal, State, and local bomb squads to defeat and mitigate terrorist devices. In collaboration with military, Federal, State, and local agencies, the IDD subgroup identifies and prioritizes multi-agency user requirements through an ongoing process. A representative from the Federal Bureau of Investigation's Bomb Data Center chairs the Subgroup.

## Focus Areas

The IDD subgroup focus areas reflect the joint priorities of military and civilian responders. During FY 2005, these focus areas were:

### Access & Diagnostics

Develop advanced technologies for diagnostic analysis of IEDs in the areas of improved tools and equipment. Develop technologies to access and accurately locate and/or identify components and composition within an improvised terrorist device to facilitate timely response and device neutralization.

### Defeat

Develop advanced technologies to defeat IEDs, VBIEDs, and improvised CBRN dispersal devices. Develop low-cost solutions that are readily available to the bomb squad community. Increase stand-off capabilities, reduce collateral damage, and provide precision disruption and disablement capabilities and techniques.

### EOD Tools

Develop improved tools and equipment to increase the safety and effectiveness of EOD and bomb technicians during a response. Enhance command and control and situational awareness. Improve tactical and personal protective equipment and other critical technologies to counter emergent explosive threats.

### Information Resources

Develop information resources and delivery systems to enhance response capabilities. Provide equipment performance evaluations, database resources, operational response technology information, and automated information systems to improve tactical and operational response capabilities.

# Improvised Device Defeat

### Remote Controlled Vehicles and Tools

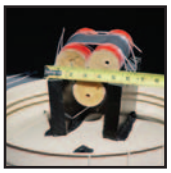
Develop technologies to improve the performance and reliability of robotic systems for the bomb technician. Develop advanced robotic platforms with improved manipulation capabilities, control systems, navigation technologies, payloads, and communications. Advance TSWG's Common System Architecture, the foundation of these systems, which for the first time enables all robotic components, regardless of the developer, to be "plug-and-play". Develop technologies that allow bomb technicians to conduct as much of their mission as possible by remote means.

## Selected Completed Projects

### Tactical Timed Firing Device

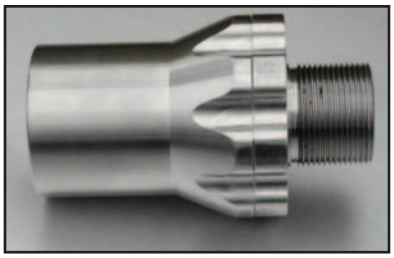

The Tactical Timed Firing Device (TTFD), developed by the Idaho National Laboratory, provides military EOD and civilian bomb disposal technicians a small, reliable, multi-use timed firing device to initiate energetic charges and tools. The device is capable of firing multi-sized shock tube, electrical blasting caps, or electrically primed cartridges. The TTFD can be ready for use in under a minute, uses standard battery power, and operates in extreme climactic conditions. Additionally, the TTFD provides an alternative to radio-frequency (RF) remote firing devices in situations where RF transmissions are prohibited. Requests for additional information should be sent to iddsubgroup@tswg.gov.

### Scalable Disruptor




Passenger cars, vans, tractor-trailer rigs, and tanker trucks have been effectively used to conceal, transport, and deliver large quantities of explosives in terrorist attacks. In cases where a VBIED can be identified and isolated before it detonates, bomb squads require a system capable of rapidly penetrating, cutting, and/or dismantling the vehicle structure and dispersing/disrupting the device without initiating it, all in a single operation. The scalable vehicle bomb disruptor developed by Applied Research Associates, Inc. is a system based on commercial-off-the-shelf plastic containers of various sizes and commercial explosive materials readily available to State and local bomb squads. The tamped detonation wave-shaping device results in a reduction of explosive mass and therefore reduced collateral damage. Fabrication information and operational guidance is available on CD-ROM for distribution to accredited bomb squads. Requests for copies of the CD-ROM should be sent to iddsubgroup@tswg.gov.

# Improvised Device Defeat

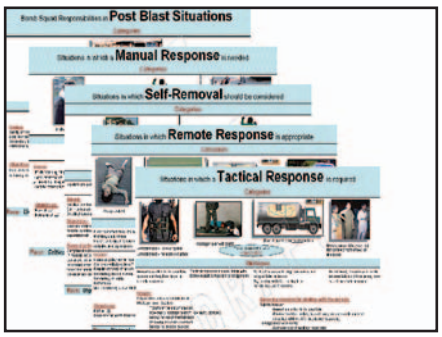


### Recoil Reduction Adapter Characterization

Bomb disposal technicians use robotic platforms to remotely position and fire explosively actuated disrupters against IEDs to access or defeat these devices. The high recoil forces of these disrupters have caused damage to the manipulator system of the robotic platform when fired. TSWG sponsored the evaluation of the Recoil Reduction Adapter (RRA), developed by the manufacturer of the Percussion Actuated Non-electric (PAN) disruptor. NAVEOTECHDIV testing verified that the RRA reduces the recoil force of the PAN by varying degrees, dependent on the type of round fired, and lessens the potential for damage to the robotic platform used to fire the disruptor. Testing also identified problems with certain PAN rounds, and the manufacturer of the rounds voluntarily took measures to resolve these. The final test report is available to the bomb disposal community to assist in their selection of rounds when using the RRA. Requests for additional information on the test report should be sent to iddsubgroup@tswg.gov. Requests for information on the RRA should be sent to Ideal Tool & Manufacturing Co., Inc. at terrell@idealtool.net.

### Radio Frequency Shielded Blackout Tent

The increasing threat of terrorist use of radio-controlled improvised explosive devices (RCIEDs) has highlighted the bomb disposal community's need for a means to isolate suspect RCIEDs from external influences. TSWG evaluated a series of rapidly deployable, multi-configuration RF-shielded enclosures that use patented BEMA RF shielding technology and are available through TEMI Support Services, LLC. These enclosures have been verified to afford bomb technicians a level of protection in dealing with radio-controlled devices. Additional information on these enclosures can be obtained by contacting TEMI at 888-797-2362.




### Suicide Bombers Countermeasures Workshop

TSWG, DHS, and FBI sponsored a suicide bomber countermeasures workshop to provide tailored guidance to bomb technicians on responding to suicide bombers. During this workshop, representatives from the bomb disposal community developed categorizations of suicide bombers and recommended response strategies. Participants at the annual Bomb Squad Commanders Conference reviewed these recommendations, which were adopted for inclusion in the 2005 National Strategic Plan for U.S. Bomb Squads. Accredited bomb technicians requiring further information can log in to the National Bomb Squad Commanders Advisory Board Web site at http://www.nbscab.org.

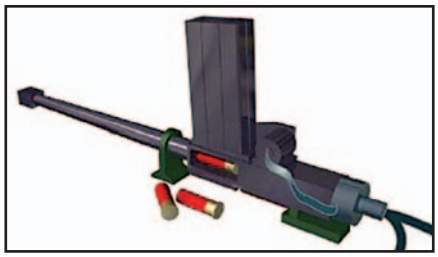
## Selected Current Projects

### Multiple IED Disruption System

The increased use of IEDs, specifically in Iraq and Afghanistan, is a significant challenge to military EOD forces. Operating in an extremely hostile environment has forced changes in traditional EOD

# Improvised Device Defeat

tactics and procedures in order to employ single-entry measures to minimize time-on-target during incidents and exposure of personnel and resources to risks. These new tactics and procedures have identified a need for a disruptor system capable of engaging multiple targets. This project will develop a platform-independent disruption system to enable multiple disruptions (4-10) during a single sortie. The system will be lightweight and easily affixed to current and future RCV platforms and will use existing RCV electronic and RF architecture, without requiring costly upgrades by the manufacturer of that system.



### Multi-Purpose Collapsible EOD Cart

The increased possibility of multiple threats requires that bomb technicians be prepared with an array of diagnostic and render-safe equipment to disable or disrupt these threats quickly and safely. Compounding the situation, personal protective gear is always required and can hinder the speed at which the bomb technicians can deliver the tools from the staging area to the deployment position. Technicians need the means to transport the equipment required for response, including into close-quarter areas. A multi-purpose cart is being developed to carry all the necessary EOD equipment to quickly diagnose, access, and disable threats; adapt to aid in the application of render-safe techniques; and function as a gurney in the event of casualties. The cart will be deployable using both manual and robotic means and will be constructed of material that reduces the risk of fragmentation in the event of device detonation.


### Robotic Power Backup for Current RCVs

Specialized robots are being used more frequently to minimize the exposure of bomb technicians when dealing with suspect IEDs. These robots are often required to operate for extended periods of time under adverse conditions. During such operations, the internal DC battery power supply can be depleted to the point of jeopardizing or interfering with the robot's operational capability. This project will develop a common backup system for current RCVs that will be capable of providing a reserve power supply during unexpected battery failure. This system will be designed to automatically switch on when main battery failure occurs and will provide enough power for the operator to recall the robot to a safe area.

### Rapid Access Neutralization Tool

Military EOD and civilian bomb technicians need a means to remotely disable critical components of vehicle bombs. Specifically, technicians need to remotely gain access to and disable select targets in inaccessible locations. The Rapid Access Neutralization Tool will provide a remote, robotically deployed disablement system capable of disrupting the circuitry of a VBIED without detonating the main explosive charge, thereby averting the damage potential of the vehicle bomb.

# Improvised Device Defeat

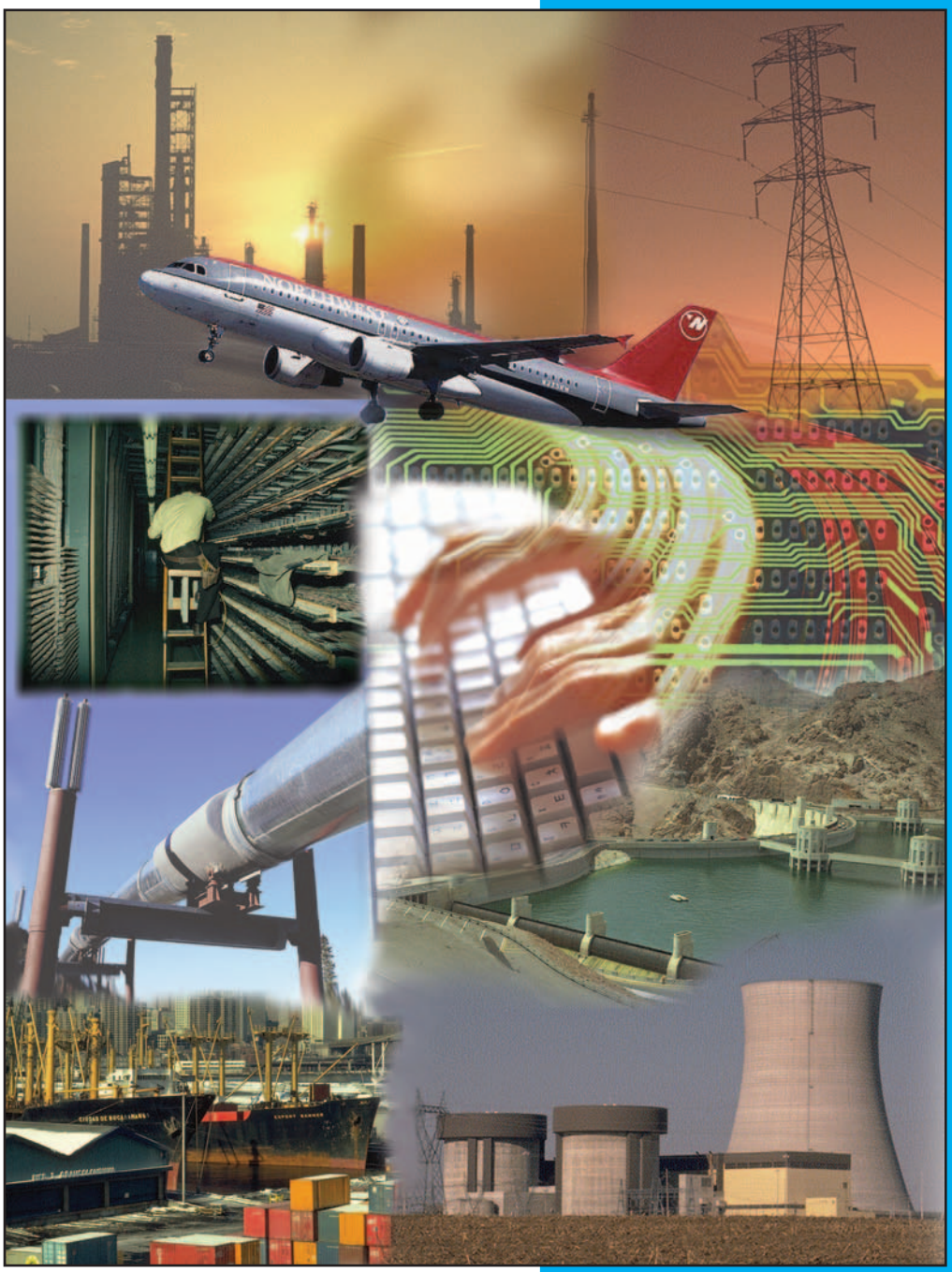
### Critical Incident Response Technology Seminars

Critical Incident Response Technology Seminars (CIRTS) bring together various subject matter experts, bomb squad technicians, and SWAT members at regional seminars held throughout the United States. Participants are introduced to technologies, capabilities, and intelligence sources focused towards dealing with the threat of IEDs, VBIEDs, and suicide bombers. CIRTS events also include hands-on application of robotics used against vehicles to access and neutralize triggering systems and various VBIED access and disruption charges. These seminars are crucial for identifying shortfalls in State and local bomb squad capabilities and preparations for future threats.

### Contact Information

iddsubgroup@tswg.gov

# Infrastructure Protection



# Infrastructure Protection

## MEMBERSHIP

**Environmental Protection Agency**

**Nuclear Regulatory Commission**

**U.S. Department of Agriculture**
FS

**U.S. Department of Defense**
DTRA, NSA, USA (CE), USAF (OSI), USMC (MCNOSC), USN (NCIS, NSWC)

**U.S. Department of Energy**
OEA, SO

**U.S. Department of Homeland Security**
FEMA, OUS-P, S&T (HSARPA), TSA, USSS

**U.S. Department of Justice**
FBI

**U.S. Department of Transportation**
FAA, Volpe

## Mission

***Identify, prioritize, and execute research and development projects that satisfy interagency requirements for the protection and assurance of critical Government, public, and private infrastructure systems required to maintain the national and economic security of the United States.***

The Infrastructure Protection (IP) subgroup works to ensure the uninterrupted service of the infrastructure systems vital to maintaining the national and economic security of the United States. These critical systems include control systems for electric power, natural gas, petroleum products, and water; telephone, radio, and television; ground, rail, and air transportation facilities; and cyber communications networks. IP research and development reflects the multivariate threat to the complex and interdependent systems, subsystems, and components of the nation's infrastructure. Solutions include conventional security measures plus those offered by emerging technologies. Representatives from the Department of Defense and the Federal Bureau of Investigation co-chair the Subgroup.

## Focus Areas

The IP subgroup focus areas reflect the prioritized requirements generated with respect to critical aspects of the nation's infrastructure. During FY 2005, these focus areas were:

### Cyber Security

Provide detection, prevention, response, and alert capabilities to counter cyber attacks and harden computer systems. Identify unforeseen vulnerabilities to complex and sophisticated information technologies. Deter criminals, terrorists, and hostile nation-states from stealing money or proprietary data, invading private records, conducting industrial espionage, or affecting vital infrastructure elements. Prevent and mitigate threats to computer networks.

### Information Analysis

Develop tools and methodologies to support analysts who can become overwhelmed by the volume, variety, and velocity of information that must be processed before decisions can be made. Enhance the storage, protection, analysis, discovery, and presentation of disparate sources of data into human-readable forms.

### Physical Protection

Standardize methodologies and decision aids for vulnerability analysis and enhanced protection of critical elements to secure the nation's infrastructure, including power generation and transmission, water supplies, and health services. Understand the dynamics of complex critical infrastructures, secure operating methodologies, and strategies to prevent and mitigate widespread failures caused by cascading and interactive network effects. Evaluate dynamic behavior models,

# Infrastructure Protection

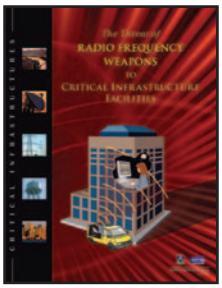
develop common standards and practices in and between critical infrastructures, and investigate system vulnerabilities to various threats.

## Selected Completed Projects

### SCADA Security Pocket Guide

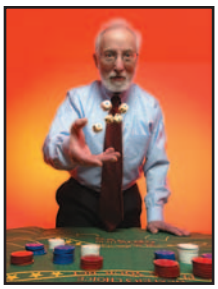

Supervisory Control and Data Acquisition (SCADA) systems are used in industrial and engineering applications to monitor and control distributed systems; many of which are vulnerable to cyber and physical attacks. TSWG teamed with Sandia National Laboratories to create the pocket guide, "Securing Your Industrial Control System", which provides a reference for enhancing the security of SCADA systems. The guide provides a comprehensive overview of industrial control system security, which includes administrative controls, architectural design, and security technology. The guide is intended for all sectors that use SCADA technology and is a resource for any asset owner trying to enhance security. Requests for the pocket guide can be sent to ipsubgroup@tswg.gov.

### Radio-Frequency Weapons Effects Characterization Pocket Guide




Radio-Frequency Weapons (RFWs) are an emerging threat on the conventional battlefield as well as a threat to critical infrastructure. The Naval Surface Warfare Center produced two reports describing the effects of RFWs. The first brochure describes the threat of RFWs and relates their use in recent history. The second is a pocket guide detailing ways to mitigate the risk of RFWs and providing tips to harden an asset against an RFW. Requests for either document can be sent to pubs@tswg.gov.

### Virus Propagation Analysis Tool



In an effort to combat the spread of viruses and malicious software, Y-12 (part of the Oak Ridge National Laboratory complex) developed the Virus Propagation Analysis Tool (VPAT). The VPAT software kit analyzes a user's network and then uses the network's characteristics to determine the best way to defend against malicious software attacks, how to recognize such attacks if and when they occur, and how to quarantine the infected parts. Requests for additional information should be sent to techtrans@tswg.gov.

### Open Source Security Tool Set


The Open Source Security Tool Set (OSST) is a suite of tools designed to assist Linux administrators in securing their systems. The Space and Naval Warfare Systems Command (SPAWAR) developed the OSST to provide security guidance in the form of two comprehensive written guides, the "Linux Security Configuration Guide" and the "Securing Web Services Guide". Following these, SPAWAR developed a Security Configuration Tool and a Security Assessment Tool to evaluate the degree of compliance to the above guidance.

# Infrastructure Protection

These tools allow organizations to both configure systems and to conduct security assessments and system validations. The above tools can be downloaded from http://fortknox.sourceforge.net.

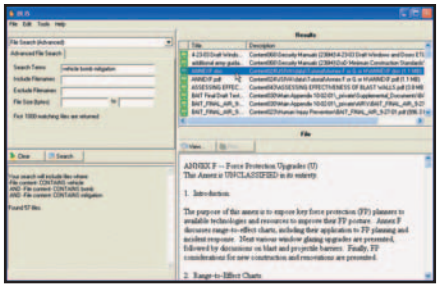
## Selected Current Projects


### Secure Aircraft Communications Addressing and Reporting System

The Aircraft Communication and Reporting System (ACARS) was initially used to accurately measure "wheels up" flight time. Over time, the amount of data flowing through the system has increased significantly and has become more sensitive. Honeywell is developing the Secure ACARS (S-ACARS) to protect this data flow. This new system will encrypt ACARS transmissions between an aircraft and a ground station.

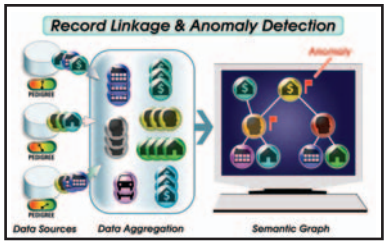

### Secure Real-Time Communications

In cooperation with the Federal Aviation Administration (FAA), Biometric Associates, Inc. is installing a Public Key Infrastructure (PKI) to demonstrate the use of biometric smart cards into a scalable, multi-agency PKI system. This pilot program will demonstrate the ability to access network, desktop, facility (physical), and FAA critical mission support system applications, as well as to evaluate interoperability with both Windows and non-Windows based platforms and applications. The system is designed to comply with Homeland Security Presidential Directive 12 as implemented by Federal Information Processing Standard 201.



### Blast Mitigation Database Conversion and Optimization

The increased use of improvised explosive devices against infrastructure highlights the need for improved information exchange. Perrault Systems, Inc. is creating the Blast Effects Information System (BLIS) database as a basis for a national program to study blast effects. The BLIS database catalogues the effects of different kinds of explosives on infrastructure and offers a convenient method of distributing the findings. The database is entering its second phase, which will convert BLIS from a stand-alone system to a Web-enabled, searchable system.




### Conflicting Data in Semantic Graphs

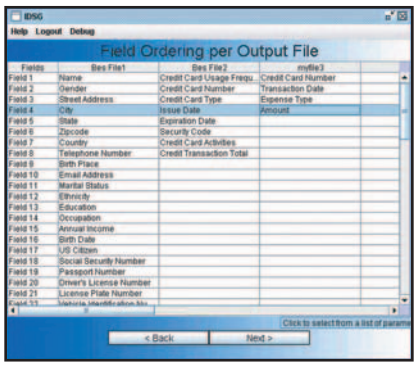
Many organizations are confronted with how to practically and reliably interpret the abundance of data now available. This is especially true for organizations that fight terrorism, since information about high-risk individuals and organizations may be deliberately modified or difficult to locate. Fetch Technologies is developing a platform that will make use of its record linkage technology to identify related database records. This technology traces the pedigree of data and establishes relationships and associations between data elements. Fetch Technologies has completed the modification of the

# Infrastructure Protection

machine learning algorithm and is investigating ways to represent semantic graphs while also allowing user input to resolve anomalous relationships among the data.

### Evaluation Testbed for Information Analysis Tools

Data-mining tools use diverse data sources to piece together evidence. A common challenge in testing these tools is the availability of input data, which can be hard to obtain because of privacy issues. Lucent Technologies is developing a synthetic data generation tool to create data for testing data-mining tools. Lucent's solution circumvents privacy concerns by generating synthetic data of sufficient quality to use for testing.




## Contact Information

ipsubgroup@tswg.gov

# Investigative Support and Forensics

# Investigative Support and Forensics

## MEMBERSHIP

**Environmental Protection Agency**
CID, NEIC

**Federal Reserve Board**

**Intelligence Community**

**National Transportation Safety Board**

**U.S. Department of Commerce**
NIST (OLES)

**U.S. Department of Defense**
AFIP, DCFL, DoDPI, USA (CID), USAF (OSI), USMC (CID), USN (NCIS)

**U.S. Department of Energy**
SO

**U.S. Department of Homeland Security**
ICE (FDL, FPS), USSS

**U.S. Department of Justice**
ATF, DEA, FBI, NIJ (NCFS, NFSTC), USMS

**U.S. Department of State**
S/CT

**U.S. Department of the Treasury**
IGTA

**U.S. Postal Inspection Service**

## Mission

***Identify, prioritize, and execute research and development projects that satisfy interagency requirements for criminal investigation, law enforcement, and forensic technology applications in terrorism-related cases.***

The Investigative Support and Forensics (ISF) subgroup implements research and development projects that provide new capabilities to law enforcement personnel, forensic scientists, and intelligence operatives responsible for investigating and interdicting terrorist incidents. Projects conducted through this group have had a major impact on forensic investigations and intelligence operations throughout the law enforcement community. A representative from the U.S. Secret Service chairs the Subgroup.

## Focus Areas

The ISF subgroup focus areas reflect the prioritized requirements of the military and civilian law enforcement communities. During FY 2005, these focus areas were:

### Crime Scene Response

Improve the quality of evidence recognition, documentation, collection, and preservation, as well as the protection of examiners from hazardous materials exposure. Train first responders and forensic examiners to handle terrorist incident scenes. Support scientific and technical efforts not assigned to other ISF focus areas.

### Electronic Evidence

Develop computer forensic hardware, software, decryption tools, and digital methods to investigate terrorism. Develop advanced methods to extract and enhance audio recordings and video images from surveillance sources. Identify computer systems and media used by terrorists and extract the maximum amount of evidence from them.

### Explosive and Hazardous Materials Examination

Improve methods for assessing the size, construction, and composition of explosive devices or other energetic hazardous materials. Identify and analyze explosive residue and other trace evidence present at blast scenes, especially those requiring rapid protection and processing, to preserve the evidentiary value.

### Forensic Biochemistry

Develop analytical methods used on biological evidence found at terrorist scenes to make identifications and extract information such as origin or age. Explore the use of DNA to identify or profile persons. Use stable isotope ratios to determine the geographic origin of organic material.

# Investigative Support and Forensics

### Friction Ridge Analysis

Improve latent print techniques used in terrorism cases. Emphasize processes involving the automation of techniques that are tedious, expensive, non-portable, or use hazardous chemicals. Address efforts to create better visualization and development of latent prints using lasers or more versatile and affordable reagents. Support better comprehension of latent prints and their molecular content, as well as the scientific validation of fingerprint examinations.

### Questioned Document Examination

Develop advanced document and handwriting analysis techniques, devise standardized identification criteria, and establish a legal scientific basis for these examinations. Investigate forgeries, tracings, disguised handwritings, and writing in different languages and character sets. Develop software to identify counterfeit documents and match documents by handwriting analysis and pattern recognition algorithms.

### Surveillance Technology

Produce new and advanced surveillance devices for law enforcement use. Examine the nature of these technologies, such as infrared, X-ray, visual, audio, and speech. Analyze the type of data derived, such as visual, aural, and digital. Determine the awareness level of the target being surveilled. Advance polygraphy and the techniques and equipment needed for the detection of deception.

## Selected Completed Projects

### Wireless Phone and Personal Digital Assistant Toolkit

Electronic data investigators need the ability to access, read, and copy stored data from wireless telephones and personal digital assistants (PDAs) while still protecting the integrity of the evidence. To assist with evidence collection, the Forensic Science Service developed a field-deployable forensic examination toolkit to extract data from wireless telephones and PDAs. The toolkit identifies the stored information on these devices and then downloads it to another computer without leaving any trace on the targeted device. Stored data that is inaccessible to the user also can be extracted. The toolkit, which is the size of a briefcase and is easily portable, is commercially available through the Logicube Web site at http://www.logicube.com.

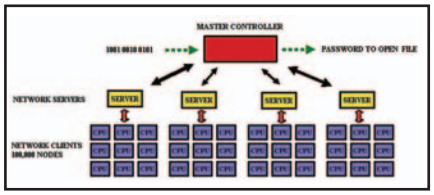
### Long-Range Non-Line-of-Sight Wireless Video Transmission System

Covert wireless video surveillance is difficult in dense urban environments. The Long-Range Non-Line-of-Sight Wireless Video Transmission System uses novel digital transmission techniques to overcome the shortcomings of current analog systems. This digital transmission system performs well in dense urban environments because it provides a video signal that overcomes high interference

# Investigative Support and Forensics

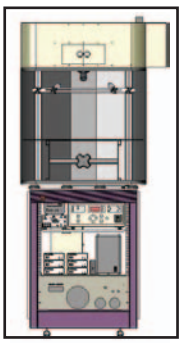
and ghost imaging. The system is interoperable with commonly used police surveillance cameras and recording equipment. This equipment is commercially available from DTC Communications, Inc. at http://www.dtccom.com/cofdm-digital-video.html.

### Counter-Encryption Tool Based on Distributive Network Processing



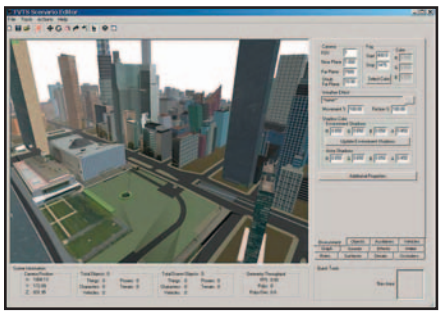

Forensic investigators are often required to break into password-protected computer systems or files with during investigations of terrorist activities. To facilitate this, AccessData Corporation developed the Distributive Network Attack, a counter-encryption tool based on distributive network processing that harnesses the unused power of up to 1000 servers and 100,000 computers on a network. The system attempts to break computer passwords by first using a dictionary approach, then analyzing internet activity, and finally by using the brute-force method. The system runs behind the scenes so that computer users on the network are not affected by its operation. This software application is commercially available from AccessData Corporation at http://www.accessdata.com/products.htm.

### Hyperspectral Contrast Imager



To help extract the maximum data from individual pieces of evidence, ChemImage, Inc. developed an advanced hyperspectral contrast imager to analyze evidence within a wider range of the light spectrum, from infrared through ultraviolet, than previously possible. In addition to providing better resolution, the imager can operate in a narrower band of wavelengths, which produces more evidentiary data. In addition to traditional paper document analysis, the imager can examine cloth, fibers, hairs, stains, biological evidence, and fingerprints. The system is compatible with the Automated Fingerprint Identification System (AFIS) and is commercially available from ChemImage at http://www.chemimage.com/ContactUs/.

### Forensic Virtual Training Simulator

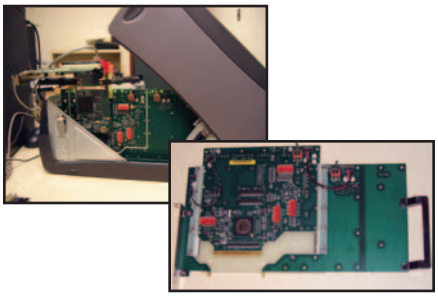


Comprehensive, realistic training for first responders can prevent terrorist incidents, save lives, and minimize damage, but training can also facilitate better evidence and intelligence collection when an incident occurs. Dynamic Animations Systems, Inc. created a forensic virtual training simulator to provide PC-based virtual training for large-scale and local threat analysis, protection planning, threat reaction and response, and forensic data search and recovery tactics. The system allows for training of individual or group tasks and has the capability to operate in a stand-alone or collaborative network mode. The simulator includes integrated application software to support features such as creating and editing scenarios, modifying the appearance of characters, operating various air vehicles, controlling groups of entities by a single participant, using virtual devices to perform forensic duties, and performing after-action review. This product is commercially available from Dynamic Animations Systems at (407) 382-2540.

# Investigative Support and Forensics

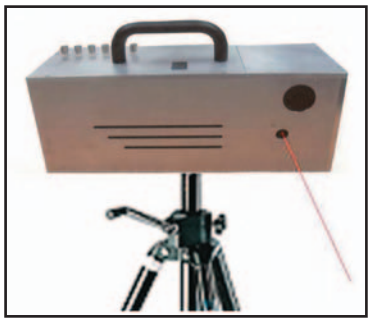
## Selected Current Projects

### RAM Capture Tool



Investigating suspected terrorists often involves extracting volatile data from a PC. BBN Technologies, Inc. is developing a RAM capture tool that connects to a running PC and extracts all of the data in the RAM and other perishable data onto another medium for storage and examination. The device will perform the data extraction without writing anything onto the hard drive or leaving any trace. The integrity of the evidence will be preserved, ensuring admissibility in court. The tool will be easy to operate, take a minimal amount of time to extract the data, and will function on multiple operating systems.

### Remote Polygraphy Using Laser Doppler Vibrometry



Traditional polygraphy tests are impractical in many environments, such as ports of entry. Law enforcement officials need techniques to quickly and surreptitiously detect deception and to prevent a suspect from using counter-interrogation tactics. Washington University in St. Louis is developing a remote polygraphy system using Laser Doppler Vibrometry (LDV). The LDV system measures physiological activity to detect deception and assess credibility. The non-contact LDV system can be used at stand-off distances of several meters. The system will include integrated eye-tracking hardware, and the system software will provide real-time data analysis. A system prototype is currently undergoing laboratory testing.

### Mobile Forensic Command Post Vehicle


Responding quickly to any location of a terrorist incident with maximum forensic capability provides the best opportunity to collect information and intelligence. The mobile forensic command post, housed in a quick-response vehicle that is also transportable by air, fills this need. The system will include satellite telecommunications and Internet access as well as forensic collection and analysis capabilities. The state-of-the-art vehicle will also contain basic living quarters and electrical self-generation to enhance its use in remote areas. The first prototype of the vehicle was used in the response to areas devastated by Hurricane Rita.

### Rapid Photo Realistic 3-D Scene Modeling System

One of the critical elements in responding to a terrorist incident is full documentation and imaging of the scene. This rapid modeling system will photograph and scan an incident scene, then produce a three-dimensional computer model of the area. The device will use COTS cameras and optics and will be rapidly deployable and easy to use. The system will be able to depict a scene as small as the interior of an automobile or as large as a 50-foot radius.

## Contact Information

isfsubgroup@tswg.gov

# Physical Security

# Physical Security

## MEMBERSHIP

**Federal Reserve Board**

**Intelligence Community**

**Nuclear Regulatory Commission**

**Port Authority of New York/New Jersey**

**U.S. Department of Defense**
CENTCOM, DARPA, DIA, DTRA, EUCOM, JCS, JFCOM, NSA, USA (PM-FPS), USAF (FPS), USMC (HQ), USN (NAVSEA)

**U.S. Department of Energy**
NNSA, SO

**U.S. Department of Homeland Security**
FEMA, FLETC, ICE (FPS), OUS-P, S&T, TSA, USCG, USSS

**U.S. Department of Justice**
ATF, FBOP, NIJ

**U.S. Department of State**
DS

## Mission

***Identify, prioritize, and execute research and development projects that satisfy interagency requirements for physical security support to protect personnel, equipment, and facilities against terrorist attack.***

The Physical Security (PS) subgroup identifies the physical security requirements of Federal agencies, both within the United States and abroad, and develops technologies to protect their personnel and property from terrorist attacks. The Subgroup develops this technology by creating prototype hardware, software, or systems for technical and operational evaluation by user agencies. A Department of Defense representative from the U.S. Naval Forces Europe chairs the Subgroup.

## Focus Areas

The PS subgroup focus areas reflect the prioritized requirements of the physical protection community. During FY 2005, these focus areas were:

### Entry-Point Screening

Develop multiple technologies and techniques to detect explosives; weapons; chemical, nuclear, and radiological materials; and other contraband on or in personnel, vehicles, vessels, cargo, and mail entering protected facilities. Solutions are intended to increase the detection rates, throughput, and safety while reducing the number of security forces required to perform the screening process.

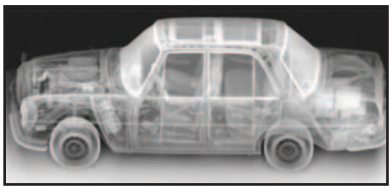
### Intrusion Detection, Assessment, and Delay

Develop improved intrusion detection systems, video alarm-assessment systems, specialized intrusion-delay barriers, and subsequent armed response capabilities for protecting outer perimeters, building perimeters, and key assets from terrorist attacks. This focus area emphasizes prototype security systems with fewer false alarms, improved reliability, higher probability of detection and assessment, lower operation and maintenance costs, and more effective response capabilities with higher probabilities for neutralizing the adversaries with reduced hazards for responding personnel.

# Physical Security

## Selected Completed Projects

### Drive-by Backscatter Van

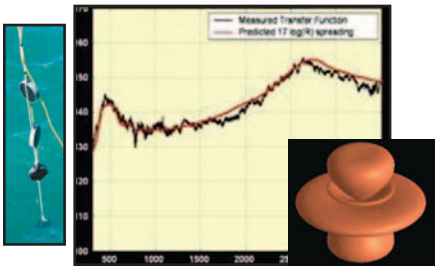


Security forces and entry-point screening personnel need the means to surreptitiously and remotely scan vehicles for explosives and other contraband. American Science and Engineering developed a utility van equipped with a backscatter X-ray imaging system to unobtrusively screen vehicles and cargo containers. An initial prototype van underwent testing in Spring 2004, and subsequent enhancements included a modification for spatial imaging correction and a remote-operations capability. The improved prototype Backscatter Van was deployed to USNAVEUR in 2005 for extended field testing. Currently more than 60 Backscatter X-Ray Vans are in operational use, and the van is commercially available from American Science and Engineering at http://www.as-e.com/products_solutions/zbv.asp.

### Advanced Vehicle/Driver Identification System

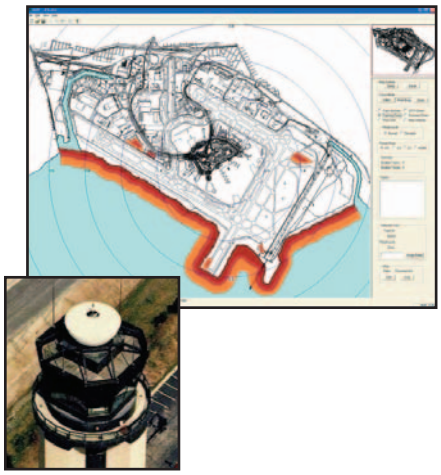
Designed to expedite the entry-point screening process, the upgraded version of the Advanced Vehicle/Driver Identification System (AVIDS) is a modular system that incorporates the use of biometrics to quickly differentiate between authorized and unauthorized personnel. In the Expeditionary Configuration that recently returned to Iraq, the Volpe National Transportation Systems Center incorporated several updates, including identifying individuals from only a single fingerprint for access control (no card required) and operating the system remotely at distances of up to 500 meters. Each AVIDS kit contains an Enrollment Center, two Entry Point Monitoring Stations, and a Data Replication Kit. Additional enhancements, including the ability to capture and transmit fingerprints during enrollment to the Biometric Fusion Center, are being developed and will be sent with units deployed in late 2005. AVIDS is licensed to Networld Exchange, Inc. (http://www.networldexchange.com); Stratech Industries, Ltd. (http://www.stratechsystems.com); and Gatekeeper, Inc. (http://www.gate-keeper.net).

### Underwater Loudhailer


Current verbal warning systems have neither the range nor the clarity to effectively contact or deter swimmers and divers approaching a restricted area. Applied Physical Sciences developed the Underwater Loudhailer to broadcast clear, intelligible speech in a variety of languages. Operated with a PDA, the Loudhailer can be deployed with existing harbor protection and coastal diver/swimmer detection systems. The system also communicates effectively in deep seas, such as around oil platforms, off-shore marine terminals, and ships at anchor. The Loudhailer emphasizes frequencies specific to underwater speech and generates a unique wave form. In FY05 Loudhailer testing showed greater than 90% intelligibility at a distance of 450 meters, a 2000% improvement over current loudhailers. In FY06 the U.S. Navy and U.S. Coast Guard will begin field trials of the prototype units. Requests for additional information should be sent to pssubgroup@tswg.gov.

# Physical Security

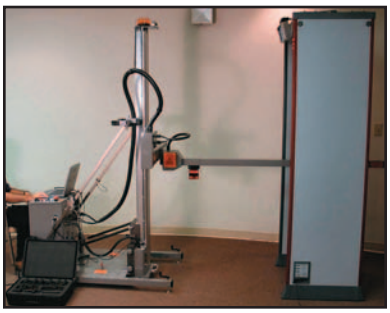


### Ground Surveillance Radar for Perimeters

Wide-area surveillance coverage at large facilities such as airports has proven costly. As an alternative, Technology Service Corporation developed a prototype perimeter security system for intrusion detection. The system was installed at a major international airport in FY05 and demonstrated that it could use the data feed from an existing FAA ASDE-3 ground surveillance radar system, which is used to track aircraft on the ground, to also meet the needs for wide-area surveillance. The surveillance system allows the operator to monitor activity beyond the perimeter, alerts the operator to potential and actual perimeter breaches, and tracks the intruders within the perimeter to help direct security forces. Additional security zones within the perimeter can be established, which allows the operator to simultaneously monitor sensitive areas such as fuel tank farms, where access generally is controlled. The airport will continue to develop and evaluate the system in FY06, after which it will be available commercially for other locations. Requests for additional information should be sent to pssubgroup@tswg.gov.

### Tactical Video Surveillance System

Military units need a perimeter security system that is easy to deploy, lightweight, compact, modular, and automated. The Space and Naval Warfare Systems Center developed the Tactical Video Surveillance System (TVSS) to provide U.S. security forces with a wireless, early-warning, long-range system using day-cameras and thermal-imagers. The TVSS uses four stations and six cameras to detect and distinguish humans and vehicles at great distances. Dual control centers allow flexibility in employment, including dedicated entry control coverage supplemented with exterior perimeter coverage. TSWG transitioned the TVSS to the U.S. Army Product Manager for Force Protection Systems (PM-FPS) in July 2004, and the system entered the DoD acquisition cycle. In FY05 PM-FPS and the U.S. Army Military Police School evaluated the system in simulated tactical environments. Based on the evaluation results, the system will be ruggedized, and PM-FPS plans to produce and field over 300 systems. Requests for additional information should be sent to pssubgroup@tswg.gov.



### Walk-Through Metal Detector Tester

While walk-through metal detectors are designed, built, and tested to rigorous Government standards prior to shipment, their operational performance currently cannot be verified. Damage during shipping or changes in calibration over long hours of use can go unnoticed. General Dynamics designed the deployable Walk-Through Metal Detector Tester to validate that metal detectors in use continue to conform to the approved Federal standards for performing forensic analyses. Three operational prototypes have been delivered for Government evaluation. The Walk-Through Metal Detector - Tester is commercially available from General Dynamics. Requests for additional information should be sent to pssubgroup@tswg.gov.

# Physical Security

## Selected Current Projects

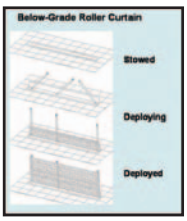
### Under-Vehicle Automated Alarm System Assessment

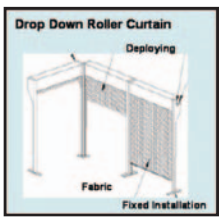
Automated under-vehicle inspection systems offer clear advantages over manual veicle inspection systems by providing improved detection capabilities and operator alarms to expedite the screening process. The remote operation of automated systems also reduces risk for security personnel. TSWG is assessing prototype image-based inspection systems that provide remote, continuous, all-weather, and day and night scanning of vehicle undercarriages. The two systems studied in 2005 identify under-vehicle anomalies by comparing the image with the automobile manufacturer's design or to the image of a previous screening. In 2006, evaluations will continue on the Stratech Industries' Intelligent Vehicle Access Control System and on the GateKeeper System, with emphasis on supporting deployed forces.

### Credentialing Technology Assessment and Demonstration

The integration of biometrics information with smart-card technology offers the potential of reducing the long lines associated with many entry control points. TSWG is assessing and demonstrating technologies that can be used for speeding access control for Government employees, contractors, and visitors entering Government facilities. The demonstration builds upon the work done by the U.S. Air Force in developing a common card reader. In FY 2006, the project will focus on matching a fingerprint to the identification presented on the smart card, then wirelessly transmitting a signal to allow or deny access.

### Breach Control Barrier System




Entry control points can often become hectic, and incompletely screened persons can quickly mix into the crowd. Vanguard Protective Technologies is developing the Breach Control Barrier System to provide a safe, fast-deploying barrier to stop personnel who violate a security screening point. Activated by security personnel, the barrier will contain the intruders in a limited area, allowing operations beyond the barrier to continue. This system will help to contain potential adversaries at security checkpoints, such as in airline terminals, courthouses, or office buildings. Fabrication and testing on three design options will be done in FY06, with production units to be tailored to specific sites. Aesthetic and safety considerations will be included in the design options so the barrier system can blend with the architectural style.

# Physical Security

### Mass Transit Surveillance and Early Warning System

World events have shown the need for fast, effective video surveillance in transportation hubs. The University of Minnesota is developing and deploying the Mass Transit Surveillance System, which is an integrated monitoring, detection, and alerting system for small and large transportation stations, such as railroad and subway stations and bus terminals. The system will distinguish, track, and display anomalous human behavior via a widely distributed set of video cameras for the identification of possible terrorist attacks. The cameras will be combined with image processing algorithms that will provide the operator with an integrated view of the site, automatic alarms of threatening actions, live and recorded video of alarm events, and the ability to respond to alarms and to control cameras. A prototype demonstration was conducted at a light rail system in Fall 2005 and will be installed at an Amtrak station starting in Spring 2006.

### Contact Information

pssubgroup@tswg.gov

# Surveillance, Collection, and Operations Support

# Surveillance, Collection, and Operations Support

## MEMBERSHIP

INTELLIGENCE COMMUNITY

U.S. DEPARTMENT OF DEFENSE
SOCOM

U.S. DEPARTMENT OF HOMELAND SECURITY
USSS

U.S. DEPARTMENT OF JUSTICE
FBI

## Mission

***Identify, prioritize, and execute research and development projects that satisfy interagency requirements supporting intelligence gathering and special operations directed against terrorist activities.***

The Surveillance, Collection, and Operations Support (SCOS) subgroup identifies high-priority user requirements and special technology initiatives focused primarily on countering terrorism through offensive operations. SCOS research and development projects enhance U.S. capabilities to conduct retaliatory or preemptive operations and reduce the capabilities and support available to terrorists. A representative from the Intelligence Community chairs the Subgroup.

## Focus Areas

The SCOS subgroup focus areas reflect the prioritized requirements of the Intelligence Community. During FY 2005, these focus areas were:

### Traditional Surveillance

Improve the quality of intelligence collection. Develop and advance capabilities for the collection and enhancement of video, imagery, and audio surveillance.

### Analytic Surveillance

Improve the means to detect terrorists by developing automated tools for terrorist identification using biometrics, pattern recognition, voice and speaker recognition, and database technologies.

### Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

Develop and improve the ability to locate, identify, and track terrorists and terrorist activities. Support programs and initiatives critical to intelligence and law enforcement operations, such as tagging, tracking, and locating; special sensors; and covert communications.

### Information Operations

Develop and improve tools to degrade, disrupt, deny, or destroy both analog and digital adversary information and information systems.

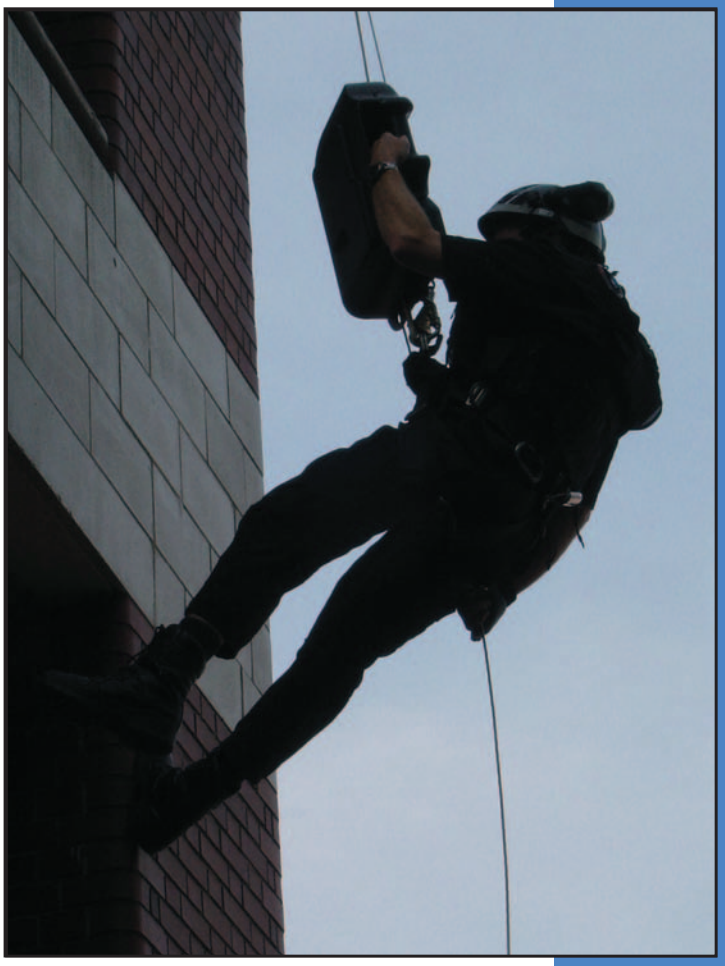
## Program Highlights

SCOS programs are classified or highly sensitive. Program requirements, the success of programs, and specific program capabilities cannot be discussed in an unclassified document.

## Contact Information

scossubgroup@tswg.gov

# Tactical Operations Support



# Tactical Operations Support

## MEMBERSHIP

**National Tactical Officers Association**

**State and Local SWAT Teams**

**U.S. Department of Defense**
SOCOM, USA (MP School)

**U.S. Department of Energy**
NNSA, SO

**U.S. Department of Homeland Security**
TSA (FAMS), USCG, USSS

**U.S. Department of Justice**
FBI (HRT), USMS

**U.S. Department of State**
DS

## Mission

***Identify, prioritize, and execute research and development projects that satisfy DoD and interagency user requirements for equipment and systems to support specialized force offensive operations directed against terrorist activities and groups. The use of non-sensitive prototype hardware for State and local law enforcement agencies is considered for product transition and commercialization.***

The Tactical Operations Support (TOS) subgroup identifies the technological needs of counterterrorist tactical operations, particularly those performed by specialized tactical forces trained for assault operations. The Subgroup supports technology development activities, which provide a foundation for subsequent advances, and the development of prototype special equipment designed to facilitate more effective execution of various tactical missions. Representatives from the Department of Defense and the Department of Energy co-chair the Subgroup.

## Focus Areas

The TOS subgroup focus areas reflect the prioritized requirements of offensive counterterrorism forces. During FY 2005, these focus areas were:

### Advanced Imaging Systems

Develop systems that improve reduced-visibility imaging in all operating environments. Provide systems that obtain high-quality images under reduced-lighting conditions and that enable tactical forces to operate more effectively.

### Specialized Access Systems

Develop technologies to assist tactical assault forces in accessing objectives, evaluating tactical options, and supporting efficiency in operations, while providing added safety for personnel.

### Chemical and Radiation Detectors

Develop chemical and radiological detection instruments that are specifically designed to support the tactical user in the field. Design systems that are smaller, lighter, more robust, and more covert than conventional technologies. Coordinate these efforts with the CBRNC subgroup.

### Offensive Systems

Develop equipment and systems to enhance the effectiveness of small offensive tactical teams in specialized operations.

# Tactical Operations Support

**Tactical Communications Systems**
Develop flexible and enhanced communications capabilities for tactical forces. Emphasize reducing the size of equipment and improving operator mobility and efficiency.

**Special Weapons and Tactics (SWAT) Support Systems**
Develop technologies to satisfy interagency operational requirements for advanced SWAT equipment and systems to combat terrorism.

## Program Highlights

TOS programs are classified or highly sensitive. Program requirements, the success of programs, and specific program capabilities cannot be discussed in an unclassified document.

## Contact Information

tossubgroup@tswg.gov

# Training Technology Development

# Training Technology Development

## MEMBERSHIP

ENVIRONMENTAL PROTECTION AGENCY

INTERAGENCY BOARD

NATIONAL BOMB SQUAD COMMANDERS ADVISORY BOARD

NATIONAL VIRTUAL TRANSLATION CENTER

U.S. DEPARTMENT OF AGRICULTURE
APHIS

U.S. DEPARTMENT OF DEFENSE
JFCOM, OUSD (P&R), PFPA, SOCOM, USA (MANSCEN, TRADOC, USAR), USMC, USN

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
FDA

U.S. DEPARTMENT OF HOMELAND SECURITY
FLETC, OUS-P, S&T, TSA, USCG, USSS

U.S. DEPARTMENT OF JUSTICE
NIJ

## Mission

***Identify, prioritize, and execute projects that satisfy interagency requirements for the development and delivery of combating-terrorism-related education, training, and mission performance support products and technologies.***

The Training Technology Development (TTD) subgroup delivers training and training technologies to increase mission readiness and enhance operational capabilities in the combating terrorism community. The strategy behind the mission is to integrate and leverage Advanced Distributed Learning (ADL) technologies to deliver high-quality education and training in the medium best suited to the users' needs and requirements. Representatives from the Department of Defense and the Department of Homeland Security co-chair the Subgroup.

## Focus Areas

The TTD subgroup focus areas reflect the prioritized requirements of the military and civilian combating-terrorism communities. During FY 2005, these focus areas were:

### Delivery Architectures

Develop new, advance emerging, and enhance existing content- and knowledge-management technologies. Develop software and hardware technologies to deliver education and training to combating-terrorism personnel. Distribute on-demand, customized training to the end user.

### Advanced Distributed Learning

Develop computer-based combating terrorism training courses and the advanced tools, techniques, and guidelines required to produce them. Integrate computer-based delivery technologies with terrorism training materials to increase the quality, effectiveness, and accessibility of training.

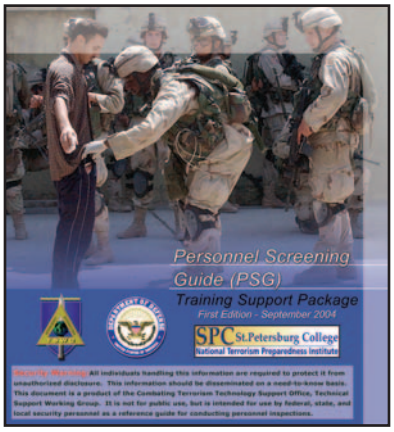
### Training Aids, Devices, and Simulations

Develop training support products and virtual training environments to support mission performance and increase mission readiness. Develop training support packages for TSWG products, incorporate exercise simulations into ADL technologies, and provide simulants for training aids.

# Training Technology Development

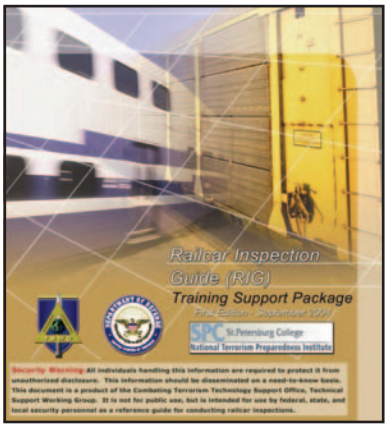
## Selected Completed Projects

### Personnel Screening Guide Training Support Package




Since 9/11, security and checkpoints at major gatherings, locations of high symbolic value, and overseas facilities have increased. The Personnel Screening Guide (PSG) Training Support Package (TSP), developed by the National Terrorism Preparedness Institute at St. Petersburg College, provides instruction on preparing security and response personnel and other emergency, government, and public service organizations responsible for screening people who may pose a terrorist threat. This TSP supplements information contained in the PSG developed by TSWG's Physical Security subgroup and should be applied in conjunction with previous training, experience, and standard procedures and policies. The PSG Training Support Package provides information on identifying suspicious individuals, completing a proper interview, and conducting searches on both the individual and personal belongings. The Training Support Package includes an instructor manual, student manual, video support segments, and a train-the-trainer video. The PSG training guide has been transitioned to the Government Printing Office, and product and procurement information is available at http://www.tswg.gov/tswg/Prods_Pubs/PSG_TSP.htm.

### Railcar Inspection Guide Training Support Package



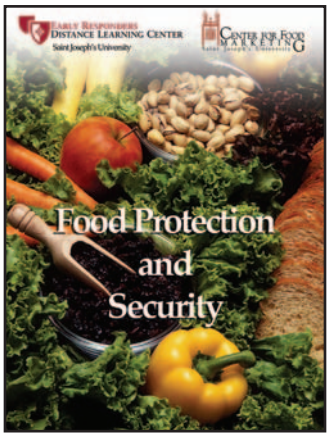

Security personnel and other emergency, government, and public service organizations are increasingly responsible for assessing, screening, and inspecting railcars for improvised explosive devices, weapons of mass destruction, and other contraband. The Railcar Inspection Guide (RIG) Training Support Package (TSP), developed by the National Terrorism Preparedness Institute at St. Petersburg College, provides tactics, techniques, and procedures for preparing security personnel for these inspections. This training package supplements information contained in the RIG developed by TSWG's Physical Security subgroup and should be applied in conjunction with previous training, experience, and standard procedures and policies. The RIG training package guides participants through three units of training: Suspicious Indicators, Interviewing, and Railcar Search. The TSP includes an instructor manual, student manual, video support segments, and a train-the-trainer video. The RIG training guide has been transitioned to the Government Printing Office, and product and procurement information is available at http://www.tswg.gov/tswg/Prods_Pubs/RIG_TSP.htm.

### Specialized Search Dog Training

Specialized search dogs (SSDs) are used to search all types of urban and rural areas, including buildings, routes, bridges, caves, and miscellaneous structures. An SSD is required to be steady under gunfire and will accept movement by all types of motor vehicles, ships, helicopters, and other aircraft. In collaboration with the U.S. Army, Concurrent Technologies Corporation developed the Specialized Search Dog training program to provide effective

# Training Technology Development

methods for training military search dogs and their handlers. Based on the United Kingdom's Arms Explosives Search course, the SSD training program is a 19-week course that trains search dogs on being fully obedient while both leashed and unleashed and under all operational conditions. The course also trains SSDs to detect firearms, ammunition, explosives, and other objects associated with bomb-making equipment. Requests for additional information should be sent to ttdsubgroup@tswg.gov.




### Food Protection and Security Training

The Food Protection and Security training program provides a curriculum for food management personnel and first responders to recognize, minimize, and manage the threat of terrorist activities across the farm to table continuum. The eight training modules focus on critical issues, including an introduction to food security and terrorism, food security risk assessment, food supply chain traceability, food security risk communication, food security risk management, food security law, securing our global food supply, and leadership in times of crisis. The courses are available individually or as a certificate program through the developer, the Early Responders Distance Learning Center at Saint Joseph's University. Currently, the program is available in Web-based, CD-ROM, and classroom delivery formats. The individual courses are free to Federal, State, and local employees who would like to participate without earning continuing education credits. Course information is available at http://erdlc.sju.edu/education-course.php?group_id=3.

## Selected Current Projects

### Scenario-Based Interactive Exercise Simulation

The Combating Terrorism (CbT) community requires capabilities and technologies that increase training opportunities while reducing travel and training costs. Applied Marine Technology, Inc. and Advanced Interactive Systems, Inc. are developing an exercise simulation that builds upon work previously funded by TSWG. The project is integrating simulation technologies (e.g., geo-specific synthetic environments, virtual reality, first-person interactive simulations, etc.) delivered via computer networks into current CbT training and exercise programs. The interactive exercise will provide trainers and operational personnel with a simulation-authoring capability and a network-capable simulation environment to supplement CBRNE planning, mission rehearsal, and table-top and full-scale exercises.

### Alert and Education Tool for Medical Professionals

Medical professionals require timely delivery of alerts and pertinent information to effectively respond to a terrorist event. The West Virginia High Technology Consortium Foundation is developing an Alert and Education Tool for Medical Professionals, which will provide an Internet portal that enables Federal, State, and local health agencies to multicast relevant alerts and educational modules through

# Training Technology Development

existing health community channels. The automated alerts and broadcasts will be Web-based and will occur in a near real-time basis. The timely delivery of alerts and associated educational material will allow the medical community to effectively respond to chemical, biological, and radiological threats by ensuring that the most current treatment methods and procedures are followed.

### Authoring Tool for Advanced Distributed Learning 3-D Simulations

Rapid response to CBRN threats requires that Federal, State, local, and military emergency responders receive in-depth training on a variety of complex equipment. Vcom3D, Inc. is designing and developing an advanced distributed learning authoring tool to create simulation-embedded Web-based and CD-based equipment training. The authoring tool will enable the integration of 3-D, 360-degree rendering and simulation into Web-based and CD-based training that is level-three interactive and that conforms to Shareable Content Object Reference Model (SCORM) 2004.

### Portable Chemical/Radiological Simulant Training Kit

Currently available chemical and radiological training kits do not fully meet the training needs for the CBRN community because many lack the fidelity of the desired agents' physical properties. Clean Earth Technologies is designing and testing a prototype portable chemical/radiological stimulant training kit, along with accompanying training aid protocols for use in decontamination training exercises. The simulant kit will also offer a commercial off-the-shelf ultraviolet light detector for simulants with fluorescent taggants and a photoionization detector to identify the location of contamination.

### Management of Agricultural Terrorism


A large-scale outbreak of an animal disease such as Foot and Mouth would challenge the response resources of the United States. The ability to enact an immediate and appropriate response would be crucial to minimizing the impact of an outbreak. To provide training on managing an agricultural incident, the Early Responders Distance Learning Center at Saint Joseph's University is developing a six-module training program on topics including: Introduction to Animal Health Emergency Management; Principles of the Incident Command System; Introduction to Agriculture and its Industries; Animal Pathogens - Pathways of Introduction; Disease Recognition, Reporting and Awareness; Disease Response Mechanisms and Bio-security; and Recovery - Animal Support Response. Anchoring themes in each module are communication, coordination, and functional roles at the Federal, State, and local levels. The courses will initially be open to USDA personnel and will be available starting in May 2006.

## Contact Information

ttdsubgroup@tswg.gov

# VIP Protection

U.S. Department of Defense

# VIP Protection

## MEMBERSHIP

**U.S. Capitol Police**

**U.S. Department of Commerce**
NIST (OLES)

**U.S. Department of Defense**
USA (SSC, TACOM)

**U.S. Department of Energy**
SO

**U.S. Department of Homeland Security**
USSS (SSD, TSD)

**U.S. Department of Justice**
NIJ

**U.S. Department of State**
DS

## Mission

***Identify, prioritize, and execute research and development projects that satisfy interagency requirements for equipment and systems that alert and prevent attacks on VIP protectees. This includes hardware and tools that provide security to both the VIPs and their protectors. Inherent in this development is additional emphasis on life safety and emergency response equipment.***

The VIP Protection (VIP) subgroup develops prototype hardware, systems, personnel protection equipment, and reference tools, as well as standards that support greater security for VIPs. To be effective, personnel who are charged with the safety of these VIPs must also have protective equipment to prevent injury and tools to improve their effectiveness. VIP projects deliver new tools and technologies to Federal, State, and local law enforcement protection details in hazardous combat-like environments and to the military. A representative from the United States Secret Service chairs the Subgroup.

## Focus Areas

The VIP subgroup focus areas reflect the prioritized requirements of the personnel protection community. During FY 2005 these focus areas were:

### Vehicle Protection and Performance

Improve the safety and effectiveness of armored vehicles to protect passengers. Develop upgrades to vehicle systems to enhance the performance and reliability of the vehicles in a broad range of operational environments. Support the validation of existing designs against specific threats.

### Transparent Armor Development

Develop and validate tools that will predict performance and support advanced design of transparent armor. Evaluate and design technologies to protect against a broad range of threat projectiles. Develop advanced lightweight transparent armor to provide substantial reductions in the weight and thickness necessary to obtain the required protection.

### Individual Protection Systems

Develop and improve methods and equipment to protect personnel assigned to VIP details. Transition appropriate technologies to law enforcement officers. Improve the performance of body armor and understand its limitations (e.g., ballistic and thermal). Provide associated systems to improve comfort and effectiveness for the wearer. Develop technologies to identify situations where protection personnel and their VIPs need additional support.

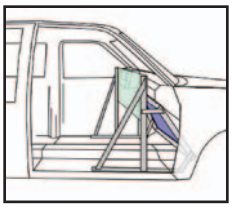
# VIP Protection

### Emerging Threats
Develop methods and systems to identify, prevent, or defeat potential attacks from remote areas. Develop technologies to identify potential sniper or remote attacks and alert users. Improve methods to provide threat-locating information and develop appropriate countermeasures.

### VIP Installation Protection
Develop threat identification and warning technologies for potential threats directed against critical installations occupied by senior government officials. Identify appropriate countermeasures to enhance a facility's safety during terrorist actions.

## Selected Completed Projects

### Armored Passenger Vehicle Guidelines
Evaluating armored passenger vehicles (APVs) is difficult for procurement personnel because of the lack of reliable performance standards for APVs. Parallel project teams from Idaho National Laboratory, QinetiQ, General Testing Laboratories, and Applied Research Associates developed guidelines prescribing the performance criteria for APVs that can be used by vendors and procurement personnel. These guidelines cover several key areas, including ballistic protection, blast protection, optical performance of transparent armor, and overall performance of APVs. Requests for additional information should be sent to vipsubgroup@tswg.gov.

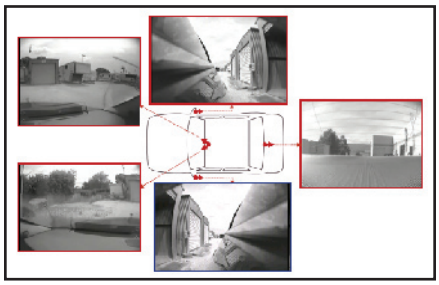


### Deployable Armor System
Critical assets and valued personnel need protection against direct attacks, particularly from weapons fire. Dynamic Defense Materials developed the Portable Armor Wall System (PAWS) that enables rapid set-up and protection against threats ranging from small to heavy ballistic calibers and limited blast. The system can be configured to provide temporary protection from armor-piercing rounds up to .50 caliber. The modular design makes it easy to assemble without tools, in configurations that meet rapid deployment requirements. The sections as packaged are light enough for a single person to lift. Additional information on PAWS is available at http://www.ddmat.com/DDM_PRODUCTS.htm.

## Selected Current Projects

### Laser Detection - Smart Glass
The ability of snipers to target VIPs through glass is not entirely mitigated by the use of transparent armor. Protection details need a system that warns of potential sniper activity by detecting the use of targeting or surveillance lasers. Applied Research Associates is developing a transparent detection film layer that can be placed on the inside of a window to detect the presence of a laser beam and issue a threat alarm to protective details.


# VIP Protection



## Covert Vehicle Tamper Detection

To improve the protection of VIPs, their vehicles need to be monitored for evidence of tampering, of having explosive devices or tracking devices attached, or of having been sabotaged in some other manner. Applied Research Associates is developing a covert vehicle tamper detection system to alert personnel of potential tampering with a vehicle, specifically the placement of IEDs or tracking devices. This system will capture potential tamper events, provide a warning, record critical details of events, allow post-event analysis of the event, and support future training exercises.

## Instantaneous Personnel Protection System

The ability to intercept weapons fire could significantly increase the level of protection available to VIPs. Southwest Research Institute and the University of Nevada at Las Vegas (UNLV) are developing the Instantaneous Personnel Protection System (IPPS), an unobtrusive automated bullet detection and countermeasure system that is capable of erecting a protective shield in a bullet's path before it reaches its target. The IPPS uses Doppler radar to detect an incoming ballistic threat and immediately deploys a ballistic shield to protect the subject. Southwest Research Institute is developing the shield and deployment mechanism, while UNLV is developing the ballistic detection system.

## Counter MANPADS Airspace Protection System

Man-Portable Air Defense Systems (MANPADS) in the hands of terrorists pose a significant threat to civilian and military aircraft, particularly during take-off and landing operations. General Dynamics is developing a ground-based counter-MANPADS system that can be rapidly deployed to high-risk areas to protect all operating aircraft. The system will detect the launch of a threat and activate a laser countermeasure to disrupt the missile guidance, preventing terminal homing of the incoming missle.


## VIP Security Kit

The danger posed by terrorism and espionage increases when VIPs travel away from fixed and easily controllable environments. Security details must be able to detect attempted intrusions into hotels or other facilities where VIPs are temporarily residing. Security personnel require an easily installable, flexible, and integrated security kit that can remotely monitor temporary sites. Applied Research Associates is developing an integrated VIP Security Kit that alerts protective details of potential security intrusions in a wide range of operating environments and installations sites. The system will be able to record surveillance data, providing a detailed record from all sensors during an incident, and to provide post-event analysis.

## Contact Information

vipsubgroup@tswg.gov

# TSWG Program Support

# Technology Transition

The TSWG charter identifies technology transition assistance throughout the development cycle as essential to supporting national combating terrorism objectives. TSWG has thus institutionalized the technology transition process into every aspect of its R&D programs. TSWG requires that every proposal received address technology transition as a principal task and that each new project include a technology transition plan. A dedicated technology transition manager works with TSWG developers to prepare the plans and to address the issues associated with a successful transition to production, such as:

- Management of intellectual property (patents, trademarks, copyrights, trade secrets, and licensing);
- Market assessments;
- Environmental, safety, and health issues;
- Liability risk reduction and consideration of SAFETY Act Applications;
- Security;
- Regulatory restrictions and export control (military and commercial);
- Test and evaluation, including independent operational testing by users;
- Transition to production, including partnering, investment capital, and licensing; and
- Operational suitability and operational support.

A number of administrative technology transition tools and methodologies are used to assist the developer with resolving issues, such as:

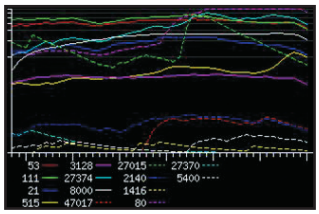
- Commercialization assessments and plan formats;
- Publication of handbooks and special primers;
- Non-disclosure agreements;
- Provisional patents;
- Liability risk reduction techniques;
- Tailored license application forms and licensee/partner selection board assistance;
- Technical data and software package management techniques;
- Federal Business Opportunity announcements;
- General Services Administration (GSA) and Defense Logistics Agency (DLA) listing assistance; and
- Licenses and Cooperative Research and Development Agreements (CRADAs).

A disciplined process; available assistance; and teamwork among project manager, technology transition manager, and developer are the keys to the rapid acceleration of the complicated process of moving many prototypes to production. For additional information, see the Technology Transition section of the TSWG Web site, http://www.tswg.gov.

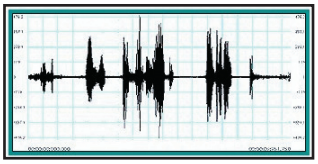
# Technology Transition

**Drink Tube Design Available to Manufacturers of Protective Masks**

**Peroxide Explosives Tester**




**Alert Trend Change Detection Tool**



**Improved Audio Enhancement Toolkit for Forensic Analysis**

**Bio Decontamination Foam; Effective Against Anthrax Contamination**


**Radiation Biodosimetry Assessment Tool -- Decision Support Software For Emergency Responders**

Examples of TSWG projects currently in transition.

# TSWG 2005 Meetings and Conferences

The following is a list of selected meetings and conferences sponsored in whole or in part by TSWG in 2005.

**Jan. 27-28**
**National Conference on Environmental Sampling for Bio-Threat Agents**
The DoD Joint Program Executive Office, DHS, and TSWG sponsored this conference to create a forum for dialogue among government, industry, academia, and first responders to address critical issues in environmental sampling, review current sampling methods and research, share lessons learned from recent events, and showcase emerging technologies.

**Feb. 21-25, May 30-June 3, July 18-22, Aug. 9-12, Sept. 19-23, and Oct. 17-21**
**Critical Incident Response Technology Seminars (CIRTS)**
CIRTS brings various subject matter experts directly to bomb technicians and SWAT members at regional seminars held throughout the United States. The seminars introduce technologies, capabilities, and intelligence sources to address the threat of IEDs, VBIEDs, and suicide bombers. Local bomb disposal units hosted individual seminars.

**Feb. 23**
**6th Advance Planning Briefing to Industry (APBI)**
TSWG announces its Broad Agency Announcement requirements for the upcoming fiscal year at these annual APBI meetings.

**Apr. 26-28**
**Force Protection Equipment Demonstration V**
The U.S. Army Product Manager (Force Protection Systems) under the Sponsorship of the Office of the Under Secretary of Defense for Acquisition, Technology & Logisitics, the Joint Staff, DOE, NIJ, and TSWG, conducted the 2005 DoD Force Protection Equipment Demonstration V (FPED V). The biannual FPED conferences provide government leaders and decision-makers with the opportunity to observe and become familiar with new COTS force protection equipment.

**June 28-30**
**Suicide Bomber Countermeasures Workshop**
TSWG, DHS, and FBI sponsored a Suicide Bomber Countermeasures Workshop to discuss characteristic of suicide bombers and to develop response strategies and standard operating procedures for mitigating suicide bombers. The outcome of the workshop was reviewed at the August 2005 Bomb Squad Commanders Conference and was approved for inclusion in the 2005 National Strategic Plan for U.S. Bomb Squads.

**Aug. 16-18**
**2005 Bomb Squad Commanders Conference**
The DHS Center for Domestic Preparedness sponsored this conference in cooperation with the National Bomb Squad Commanders Advisory Board, FBI, ATF, NIJ, and TSWG. This year's theme was "Information Technology in Support of Bomb Squads".

# TSWG 2005 Meetings and Conferences

**Aug. 23-25**
**4th International Enhanced Novel Explosives Workshop**
TSWG sponsored this workshop to bring together government and industry personnel who have an active interest in enhanced novel explosives and in mitigating these threats. The 2005 workshop focused on the dynamics of enhanced novel explosives and their range of uses, such as weaponized thermobarics, enhanced formulations, terrorist use of explosives, and the instrumentation suites used to gather and analyze data. Federal Agency partners co-hosted various sessions.

**Sept. 13; Oct. 12**
**First Responder Simulation Requirements Workshop**
TSWG sponsored this workshop to glean design and development input from knowledgeable potential end users relative to functionality requirements, technical system requirements, and training exercise scenario requirements. The target audience included first responders (trainers and trainees) and exercise controllers.

**Dec. 13-14**
**Unmanned Systems Capabilities Conference II**
TSWG and the Joint Robotics Program co-sponsored this conference to leverage the efforts of DoD and other interagency organizations in developing unmanned systems. The conference provided a forum for government program managers and users to share program information and requirements with the robotics industry and academia.

# BAA Information Delivery System (BIDS)

TSWG seeks technology solutions that address operational and technological shortfalls identified by Government agency users at least once annually. User requirements are disclosed in a solicitation format called a Broad Agency Announcement (BAA). The BAA enables the Government to solicit industry, academia, and Government laboratories for innovative research and development solutions to these requirements. The BAA is advertised in the Federal Business Opportunities at http://www.fedbizopps.gov. The FedBizOpps site directs interested bidders to the appropriate Web address where additional information for submitting a proposal is posted.

Each open BAA is always accessible through the TSWG program Web site at http://www.bids.tswg.gov. The application at this website is called the BAA Information Delivery System (BIDS). BIDS provides an electronic submission and review capability for receiving and evaluating responses to a BAA. BIDS provides a secure 128-bit encryption for proposal response uploads by prospective bidders and ensures control of proprietary bidder data.

By harnessing the technical capabilities of BIDS, TSWG increases the return on investment in counterterrorism technologies made by multiple Federal agencies to support their initiatives. BIDS continues to serve as a model for other Federal programs that seek to solicit technical proposals while eliminating the inconvenience of paper forms, the unnecessary waste in processing time, and excessive application mailing expenses.

# Appendices

U.S. Department of Defense

# TSWG 2005 Membership

## Federal Agencies

### U.S. Department of Defense

- Armed Forces Institute of Pathology
- Defense Advanced Research Projects Agency
- Defense Computer Forensics Laboratory
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Joint Chiefs of Staff
- National Security Agency
- Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict
- Office of the Deputy Assistant to the Secretary of Defense for Chemical and Biological Defense
- Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
- Office of the Under Secretary of Defense for Personnel and Readiness
- Pentagon Force Protection Agency
- Polygraph Institute
- U.S. Air Force
  - Air Combat Command
  - Air Force Electronic Systems Center
  - Air Force Research Laboratory
  - Explosive Ordnance Disposal Detachment 63
  - Force Protection System Program Office
  - Office of Special Investigations
- U.S. Army
  - 22nd Chemical Battalion (Technical Escort)
  - 52nd Ordnance Group
  - Army Research Laboratory
  - Chemical School
  - Corps of Engineers
  - Criminal Investigation Command
  - Explosive Ordnance Disposal Technical Detachment
  - Force Protection Systems
  - Maneuver Support Center
  - Military Police School
  - National Ground Intelligence Center
  - Research, Development, and Engineering Command
    - Edgewood Chemical Biological Center
  - Soldier Systems Center (Natick)
  - Tank-Automotive and Armaments Command
  - Training and Doctrine Command
  - U.S. Army Institute of Surgical Research
  - U.S. Army Reserve
- U.S. Central Command
- U.S. European Command

# TSWG 2005 Membership

- U.S. Joint Forces Command
- U.S. Marine Corps
  - Chemical Biological Incident Response Force
  - Criminal Investigation Division
  - Headquarters Battalion
  - Marine Corps Network Operations and Security Command
  - Naval Explosive Ordnance Disposal Technology Division, Marine Corps Detachment
- U.S. Navy
  - Bureau of Medicine and Surgery
  - Naval Air Warfare Center
  - Naval Criminal Investigative Service
  - Naval Explosive Ordnance Disposal Fleet Liaison Office
  - Naval Facilities Engineering Command
    - Naval Facilities Engineering Service Center
  - Naval Forces Central Command
  - Naval Health Research Center
  - Naval Research Laboratory
  - Naval Sea System Command
    - Naval Explosive Ordnance Disposal Technology Division
    - Naval Surface Warfare Center
- U.S. Special Operations Command

**Environmental Protection Agency**
**Federal Reserve Board**
**Intelligence Community**
**InterAgency Board**
**National Aeronautics and Space Administration**
**National Transportation Safety Board**
**National Virtual Translation Center**
**Nuclear Regulatory Commission**
**U.S. Department of Agriculture**
- Agricultural Research Service
- Animal and Plant Health Inspection Service
- Food Safety and Inspection Service
- Forest Service

**U.S. Department of Commerce**
- National Institute of Standards and Technology

**U.S. Department of Energy**
- National Nuclear Security Administration
- Office of Energy Assurance
- Office of Security

**U.S. Department of Health and Human Services**
- Centers for Disease Control and Prevention
- Food and Drug Administration
- National Institute for Occupational Safety and Health

# TSWG 2005 Membership

**U.S. Department of Homeland Security**

- Customs and Border Protection
- Federal Emergency Management Agency
- Federal Law Enforcement Training Center
- Immigration and Customs Enforcement
  - Federal Protective Service
  - Forensic Document Laboratory
- Office of the Under Secretary for Preparedness
- Science and Technology Directorate
  - Homeland Security Advanced Research Projects Agency
- Transportation Security Administration
  - Federal Air Marshal Service
- U.S. Coast Guard
- U.S. Secret Service

**U.S. Department of Justice**

- Bureau of Alcohol, Tobacco, Firearms, and Explosives
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Federal Bureau of Prisons
- National Institute of Justice
- U.S. Marshals Service

**U.S. Department of State**

- Bureau of Diplomatic Security
- Office of the Coordinator for Counterterrorism
- Overseas Building Operations

**U.S. Department of Transportation**

- Federal Aviation Administration
- Volpe National Transportation Systems Center

**U.S. Department of the Treasury**

- Inspector General for Tax Administration

**U.S. Postal Inspection Service**

## Legislative Branch

**U.S. Capitol Police**

**U.S. Senate Sergeant at Arms**

# TSWG 2005 Membership

## State and Local Agencies

Fairfax County (VA) Police Department
New York City Fire Department
New York City Mass Transit Authority
New York City Police Department
Port Authority of New York/New Jersey
Seattle (WA) Fire Department
State and Local SWAT Teams

## Non-Governmental Organizations

National Bomb Squad Commanders Advisory Board
National Tactical Officers Association

# 2005 Membership by Subgroup

## Blast Effects and Mitigation

**New York City Mass Transit Authority**
**Port Authority of New York/New Jersey**
**U.S. Department of Defense**
- Defense Threat Reduction Agency
- U.S. Army
  - Army Instuitute of Surgical Research
  - Army Research Laboratory
  - Corps of Engineers
    - Protective Design Center
  - Soldier Systems Center (Natick)
- U.S. Air Force
  - Air Force Research Lab
- U.S. Navy
  - Naval Facilities Engineering Command
  - Naval Health Research Center

**U.S. Department of Justice**
- Bureau of Alcohol, Tobacco, Firearms, and Explosives

**U.S. Department of State**
- Bureau of Diplomatic Security

## Chemical, Biological, Radiological, and Nuclear Countermeasures

**Environmental Protection Agency**
**Federal Reserve Board**
**Intelligence Community**
**InterAgency Board**
**New York City Fire Department**
**New York City Police Department**
**Nuclear Regulatory Commission**
**Seattle (WA) Fire Department**
**U.S. Capitol Police**
**U.S. Department of Agriculture**
- Agricultural Research Service
- Animal and Plant Health Inspection Service
- Food Safety and Inspection Service

**U.S. Department of Commerce**
- National Institute of Standards and Technology

**U.S. Department of Defense**
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Joint Chiefs of Staff
- National Security Agency
- Office of the Deputy Assistant to the Secretary of Defense for Chemical and Biological Defense
- Pentagon Force Protection Agency
- U.S. Air Force
  - Air Combat Command

# 2005 Membership by Subgroup

- U.S. Army
  - 22nd Chemical Battalion (Technical Escort)
  - 52nd Ordnance Group
  - Chemical School
  - Maneuver Support Center
  - National Ground Intelligence Center
  - Research, Development, & Engineering Command
    - Edgewood Chemical Biological Center
- U.S. Marine Corps
  - Chemical Biological Incident Response Force
- U.S. Navy
  - Bureau of Medicine and Surgery
  - Naval Air Warfare Center
  - Naval Forces Central Command
  - Naval Surface Warfare Center

**U.S. Department of Energy**
- Office of Security

**U.S. Department of Health and Human Services**
- Centers for Disease Control and Prevention
- Food and Drug Administration
- National Institute for Occupational Safety and Health

**U.S. Department of Homeland Security**
- Federal Emergency Management Agency
- Immigration and Customs Enforcement
  - Federal Protective Service
- Science and Technology Directorate
  - Homeland Security Advanced Research Projects Agency
- Transportation Security Administration
- U.S. Coast Guard
- U.S. Secret Service

**U.S. Department of Justice**
- Federal Bureau of Investigation
- National Institute of Justice
- U.S. Marshals Service

**U.S. Department of State**
- Bureau of Diplomatic Security
- Office of the Coordinator for Counterterrorism
- Overseas Building Operations

**U.S. Postal Inspection Service**

**U.S. Senate Sergeant at Arms**

## Explosives Detection

**U.S. Department of Defense**
- Defense Intelligence Agency
- National Security Agency
- U.S. Air Force
  - Air Force Electronic Systems Center
  - Air Force Research Laboratory

# 2005 Membership by Subgroup

- U.S. Navy
  - Naval Explosive Ordnance Disposal Technology Division
  - Naval Research Laboratory

**U.S. Department of Energy**
- Office of Security

**U.S. Department of Homeland Security**
- Immigration and Customs Enforcement
  - Federal Protective Service
- Science and Technology Directorate
  - Homeland Security Advanced Research Projects Agency
- Transportation Security Administration
  - Federal Air Marshal Service
- U.S. Coast Guard
- U.S. Secret Service

**U.S. Department of State**
- Bureau of Diplomatic Security

**U.S. Postal Inspection Service**

## Improvised Device Defeat

**Fairfax County (VA) Police Department**

**Intelligence Community**

**National Bomb Squad Commanders Advisory Board**
- Bloomington, Minnesota Police Department (Northern region)
- Houston, Texas Police Department (Southern region)
- Los Angeles, California Police Department (Western region)
- Philadelphia, Pennsylvania Police Department (Eastern region)

**U.S. Capitol Police**

**U.S. Department of Defense**
- U.S. Air Force
  - Air Combat Command
  - Explosive Ordnance Disposal Detachment 63
- U.S. Army
  - 52nd Ordnance Group
  - Explosive Ordnance Disposal Technical Detachment
- U.S. Marine Corps
  - Chemical Biological Incident Response Force
  - Naval Explosive Ordnance Disposal Technology Division, Marine Corps Detachment
- U.S. Navy
  - Naval Explosive Ordnance Disposal Fleet Liaison Office
  - Naval Explosive Ordnance Disposal Technology Division

# 2005 Membership by Subgroup

**U.S. Department of Homeland Security**
- Office of the Under Secretary for Preparedness
- Science and Technology Directorate
  - Homeland Security Advanced Research Projects Agency
- Transportation Security Administration
- U.S. Secret Service

**U.S. Department of Justice**
- Bureau of Alcohol, Tobacco, Firearms, and Explosives
- Federal Bureau of Investigation
- National Institute of Justice
- U.S. Marshals Service

## Infrastructure Protection

**Environmental Protection Agency**

**Nuclear Regulatory Commission**

**U.S. Department of Agriculture**
- Forest Service

**U.S. Department of Defense**
- Defense Threat Reduction Agency
- National Security Agency
- U.S. Air Force
  - Office of Special Investigations
- U.S. Army
  - Corps of Engineers
- U.S. Marine Corps
  - Marine Corps Network Operations and Security Command
- U.S. Navy
  - Naval Criminal Investigative Service
  - Naval Surface Warfare Center

**U.S. Department of Energy**
- Office of Energy Assurance
- Office of Security

**U.S. Department of Homeland Security**
- Federal Emergency Management Agency
- Office of the Under Secretary for Preparedness
- Science and Technology Directorate
  - Homeland Security Advanced Research Projects Agency
- Transportation Security Administration
- U.S. Secret Service

**U.S. Department of Justice**
- Federal Bureau of Investigation

**U.S. Department of Transportation**
- Federal Aviation Administration
- Volpe National Transportation Systems Center

# 2005 Membership by Subgroup

## Investigative Support and Forensics

**Environmental Protection Agency**
- Criminal Investigation Division
- National Enforcement Investigations Center

**Federal Reserve Board**

**Intelligence Community**

**National Transportation Safety Board**

**U.S. Department of Commerce**
- National Institute of Standards and Technology
  - Office of Law Enforcement Standards

**U.S. Department of Defense**
- Armed Forces Institute of Pathology
- Defense Computer Forensics Laboratory
- Polygraph Institute
- U.S. Air Force
  - Office of Special Investigations
- U.S. Army
  - Criminal Investigation Command
- U.S. Marine Corps
  - Criminal Investigation Division
- U.S. Navy
  - Naval Criminal Investigative Service

**U.S. Department of Energy**
- Office of Security

**U.S. Department of Homeland Security**
- Immigration and Customs Enforcement
  - Federal Protective Service
  - Forensic Document Laboratory
- U.S. Secret Service

**U.S. Department of Justice**
- Bureau of Alcohol, Tobacco, Firearms, and Explosives
- Drug Enforcement Administration
- Federal Bureau of Investigation
- National Institute of Justice
  - National Center for Forensic Science
  - National Forensic Science Technology Center
- U.S. Marshals Service

**U.S. Department of State**
- Office of the Coordinator for Counterterrorism

**U.S. Department of the Treasury**
- Inspector General for Tax Administration

**U.S. Postal Inspection Service**

# 2005 Membership by Subgroup

## Physical Security

**Federal Reserve Board**
**Intelligence Community**
**Nuclear Regulatory Commission**
**Port Authority of New York/New Jersey**
**U.S. Department of Defense**

- Defense Advanced Research Projects Agency
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Joint Chiefs of Staff
- National Security Agency
- U.S. Air Force
  - Force Protection System Program Office
- U.S. Army
  - Product Manager–Force Protection Systems
- U.S. Central Command
- U.S. European Command
- U.S. Joint Forces Command
- U.S. Marine Corps
  - Headquarters Battalion
- U.S. Navy
  - Naval Sea Systems Command

**U.S. Department of Energy**

- National Nuclear Security Administration
- Office of Security

**U.S. Department of Homeland Security**

- Federal Emergency Management Agency
- Federal Law Enforcement Training Center
- Immigration and Customs Enforcement
  - Federal Protective Service
- Office of the Under Secretary for Preparedness
- Science and Technology Directorate
- Transportation Security Administration
- U.S. Coast Guard
- U.S. Secret Service

**U.S. Department of Justice**

- Bureau of Alcohol, Tobacco, Firearms, and Explosives
- Federal Bureau of Prisons
- National Institute of Justice

**U.S. Department of State**

- Bureau of Diplomatic Security

# 2005 Membership by Subgroup

## Surveillance, Collection, and Operations Support

**Intelligence Community**

**U.S. Department of Defense**
- U.S. Special Operations Command

**U.S. Department of Homeland Security**
- U.S. Secret Service

**U.S. Department of Justice**
- Federal Bureau of Investigation

## Tactical Operations Support

**National Tactical Officers Association**

**State and Local SWAT Teams**

**U.S. Department of Defense**
- U.S. Army
  - Military Police School
- U.S. Special Operations Command

**U.S. Department of Energy**
- National Nuclear Security Administration
- Office of Security

**U.S. Department of Homeland Security**
- Transportation Security Administration
  - Federal Air Marshal Service
- U.S. Coast Guard
- U.S. Secret Service

**U.S. Department of Justice**
- Federal Bureau of Investigation
  - Hostage Rescue Team
- U.S. Marshals Service

**U.S. Department of State**
- Bureau of Diplomatic Security

## Training Technology Development

**Environmental Protection Agency**

**InterAgency Board**

**National Bomb Squad Commanders Advisory Board**

**National Virtual Translation Center**

**U.S. Department of Agriculture**
- Animal and Plant Health Inspection Service

**U.S. Department of Defense**
- Office of the Under Secretary of Defense for Personnel and Readiness
- Pentagon Force Protection Agency
- U.S. Army
  - Maneuver Support Center
  - Training and Doctrine Command
  - U.S. Army Reserve

# 2005 Membership by Subgroup

- U.S. Joint Forces Command
- U.S. Marine Corps
- U.S. Navy
- U.S. Special Operations Command

**U.S. Department of Health and Human Services**
- Food and Drug Administration

**U.S. Department of Homeland Security**
- Federal Law Enforcement Training Center
- Office of the Under Secretary for Preparedness
- Science and Technology Directorate
- Transportation Security Administration
- U.S. Coast Guard
- U.S. Secret Service

**U.S. Department of Justice**
- National Institute of Justice

## VIP Protection

**U.S. Capitol Police**

**U.S. Department of Commerce**
- National Institute of Standards and Technology
  - Office of Law Enforcement Standards

**U.S. Department of Defense**
- U.S. Army
  - Soldier Systems Center (Natick)
  - Tank-Automotive and Armaments Command

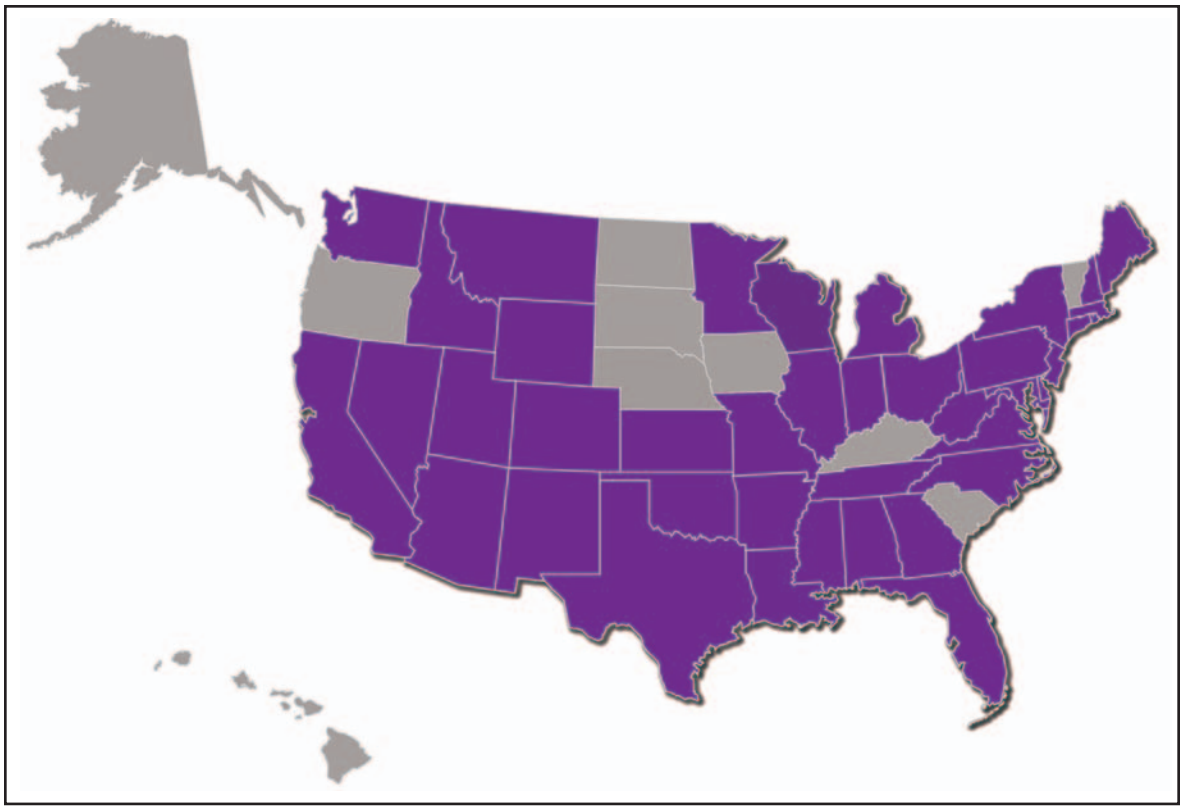
**U.S. Department of Energy**
- Office of Security

**U.S. Department of Homeland Security**
- U.S. Secret Service
  - Special Services Division
  - Technical Security Division

**U.S. Department of Justice**
- National Institute of Justice

**U.S. Department of State**
- Bureau of Diplomatic Security

# 2005 Performers



### Alabama
Auburn University, Auburn

### Arizona
Pacific Scientific, Chandler
Polymicro Technologies, LLC, Phoenix

### Arkansas
The Tekne Group, Inc., Hot Springs
University of Arkansas at Fayetteville

### California
Advanced Countermeasures Systems, Inc., Rancho Cordova
Ancore, Santa Clara
BEAR, Inc., Berkeley, CA
ComGlobal Systems, Inc., San Diego
Dynamics Technology, Inc., Torrance
GE Infrastructure–Security, San Diego
Intelligent Optical Systems, Inc., Torrance
Jet Propulsion Laboratory, Pasadena
Joint Warfare Program Office, Point Mugu
Karagozian & Case, Burbank
Lawrence Berkeley National Laboratory, Berkeley
Lawrence Livermore National Laboratory, Livermore

# 2005 Performers

Naval Air Warfare Station, Point Mugu
QPC Fiber Optic, Inc., San Clemente
Quantum Magnetics, Inc., San Diego
Rapiscan Security Products, Hawthorne
Raymat Materials, Inc., Fremont
Safe Environment Engineering, Valencia
SAIC, San Diego
Smiths Detection, Pasadena
Space and Naval Warfare Systems Command (SPAWAR), San Diego
Special Technologies Laboratory, Santa Barbara
Tactical Survey Group, Crestline
TelAir International, Rancho Dominguez
Trex Enterprises, San Diego
University of California at San Diego
WaveBand Corporation, Irvine
WFI Government Services, Newbury Park
X-Ray Instrumentation Associates, Newark

### Colorado
Applied Research Associates, Inc., Littleton
Law Enforcement Technologies, Inc., Colorado Springs
Thermo MF Physics, Colorado Springs

### Connecticut
Applied Physical Sciences Corporation, New London
Naval Submarine Medical Research Laboratory, Groton
Nextgen Fiber Optics, LLC, Dayville
United Technologies Research Center, Hartford

### Delaware
DuPont, Wilmington

### District of Columbia
BAE Systems Advanced Technologies, Inc.
International Association of Firefighters
Naval Research Laboratory
Perrault Structural Products, Inc.

### Florida
46 Test Squadron, Eglin Air Force Base
Air Force Research Laboratory, Tyndall Air Force Base
Armor Holdings, Inc., Jacksonville
Engineering Technology, Inc., Orlando
Harris Government Communications Systems Division, Melbourne
Knights Armaments Company, Vero Beach
St. Petersburg College, National Terrorism Preparedness Institute, St. Petersburg
VCom3D, Inc., Orlando

# 2005 Performers

### Georgia
Emory University, Atlanta
Georgia Tech Research Institute, Atlanta

### Idaho
Idaho National Engineering and Environmental Laboratory, Idaho Falls

### Illinois
Applied Research Associates, Champaign
Argonne National Laboratory, Argonne
Gas Technology Institute, Des Plaines
Nanosphere, Inc., Northbrook

### Indiana
Creative Business Products, Fort Wayne
Naval Surface Warfare Center, Crane

### Kansas
Kansas State University, Manhattan

### Louisiana
Louisiana State University, Baton Rouge

### Maine
Sensor Research and Development Corporation, Orono

### Maryland
Army Research Lab, Aberdeen Proving Ground
20/20 Gene Systems, Rockville
AeroSafe, LLC, Bethesda
Armed Forces Radiobiology Research Institute, Bethesda
CeLight, Silver Spring
Edgewood Chemical Biological Center, Aberdeen Proving Ground
GEOMET Technologies, Inc., Germantown
Johns Hopkins University Applied Physics Laboratory, Laurel
National Institute of Standards and Technology, Gaithersburg
Naval Air Warfare Center, Patuxent River
Naval Surface Warfare Center, Carderock Division
Naval Surface Warfare Center, Indian Head Division
Northrop Grumman Electronic Systems, Linthicum
Syntonics, Columbia
Technical Services Corporation, Silver Spring
Technology Assessment & Transfer, Inc., Annapolis
Veritas, Inc., Rockville
Zeus Technology Systems, Inc., Hanover

# 2005 Performers

### Massachusetts
American Science & Engineering, Billerica
BBN Technologies, Cambridge
CyTerra Corporation, Waltham
FLIR Systems, Inc., North Billerica
Force Protection C2 SPO, Hanscom Air Force Base
Foster-Miller, Inc., Waltham
GE Ion Track, Wilmington
iRobot, Burlington
Massachusetts General Hospital, Boston
Massachusetts Institute of Technology, Cambridge
Pulmatrix, Inc., Cambridge
Surmet Corp., Burlington
Technical Products, Inc., Framingham
The Charles Stark Draper Laboratory, Inc., Cambridge
Tufts University, Medford
University of Massachusetts at Amherst
U.S. Army Soldier Systems Center, Natick
Volpe National Transportation Systems Center, Cambridge
Woods Hole Oceanographic Institution, Woods Hole

### Michigan
Picometrix, Inc., Ann Arbor

### Minnesota
Honeywell Laboratories, Minneapolis
MTS Systems Corporation, Eden Prairie
The Mayo Clinic, Rochester
University of Minnesota at Minneapolis

### Mississippi
Mississippi State University at Starkville

### Missouri
Alliant Lake City Small Caliber Ammunition Company, LLC, Independence
Clean Earth Technologies, LLC, Earth City
Midwest Research Institute, Kansas City
University of Missouri at Rolla
Washington University, St. Louis

### Nevada
University of Nevada at Las Vegas

### New Hampshire
DTC Communications, Inc., Nashua
Globe Manufacturing Company, Pittsfield
Impact Science and Technology, Nashua
StockerYale, Inc., Salem
Wilcox Industries Corporation, Portsmouth

# 2005 Performers

### New Jersey
JeBen Photonics, Inc., Denville
JP Laboratories, Middlesex
New Jersey Institute of Technology, Newark
Sarnoff Corporation, Princeton
Structured Materials Industries, Piscataway
U.S. Army Communications-Electronics Command, Fort Monmouth

### New Mexico
Applied Research Associates, Inc., Albuquerque
Intellite, Inc., Albuquerque
Los Alamos National Laboratory, Los Alamos
MesoSystems Technology, Inc., Albuquerque
New Mexico Institute of Mining and Technology, Energetic Materials Research and Testing Center, Socorro
National Assessment Group, Albuquerque
Sandia National Laboratories, Albuquerque
SAIC, Albuquerque
University of New Mexico at Albuquerque

### New York
ACS Defense, Inc., Rome
Air Force Research Laboratory, Rome
Calspan-UB Research Center, Inc., Buffalo
Esensors, Inc., Amherst
GE Global Research, Niskayuna
IBM, Watson Research Center, Yorktown Heights
Onondaga Community College, Public Safety Training Center, Syracuse
Research Associates for Defense Conversion, Rome
Sensis Corporation, East Syracuse
Sentigen Holding Corporation, New York
State University of New York at Buffalo
Syracuse Research Corporation, Syracuse
Tactronics, LLC, Westhampton Beach
Weidlinger Associates, Inc., New York

### North Carolina
Appealing Products, Inc., Raleigh
General Dynamics–Armament & Technical Products, Charlotte
North Carolina State University, Textile Protection and Comfort Center, Raleigh
Research Triangle Institute, Research Triangle Park

### Ohio
Battelle Memorial Institute, Columbus
Northeastern Ohio Universities College of Medicine, Rootstown
Total Fire Group/Morning Pride Manufacturing, Dayton
University of Dayton Research Institute, Dayton

### Oklahoma
Nomadics, Inc., Stillwater
Southwest Research Institute, Oklahoma City

# 2005 Performers

### Pennsylvania
Carnegie Mellon University, Pittsburgh
Carnegie Mellon University, Learning Systems Architecture Lab, Pittsburgh
ChemImage, Pittsburgh
Concurrent Technologies Corporation, Johnstown
Drexel University, Data Fusion Laboratory, Philadelphia
DRS Laurel Technologies, Johnstown
Dynamic Defense Materials, LLC, Boothwyn
National Institute for Occupational Safety and Health, National Personal Protective Technology Laboratory, Pittsburgh
Optical Systems Technology, Inc., Freeport
Pennsylvania State University, University Park
Saint Joseph's University, Early Responders Distance Learning Center, Philadelphia

### Rhode Island
Naval Underwater Warfare Center, Newport

### Tennessee
Animax Designs, Inc., Nashville
BWXT Y-12, Oak Ridge
Oak Ridge National Laboratory, Oak Ridge

### Texas
Applied Research Associates, Inc., San Antonio
AptaMed, Inc., Galveston
BAE Systems Integrated Defense Solutions, Inc., Austin
Force Protection Battle Lab, Lackland Air Force Base
International Personnel Protection, Austin
Lockheed Martin Corporation, Missile and Fire Control, Dallas
Lynntech, Inc., College Station
Military Working Dog Center, San Antonio
Southwest Research Institute, San Antonio
Texas Agricultural Experiment Station, Bryan
University of Texas at Austin

### Utah
AccessData Corporation, Orem
IsoForensics, Inc., Salt Lake City
University of Utah, Salt Lake City

### Virginia
A-T Solutions, Inc., Fredericksburg
Applied Marine Technology, Inc., Virginia Beach
Avir, LLC, Charlottesville
Battelle Memorial Institute, Arlington
Defense Group, Inc., Alexandria
Dynamic Animation Systems, Fairfax
ENSCO, Inc., Springfield
Fairfax County Fire Department, Fairfax
Gatekeeper, Inc., Reston

# 2005 Performers

General Dynamics–Advanced Information Systems, Charlottesville
General Testing Laboratories, Colonial Beach
Homeland Water Security Technologies, Inc., Arlington
International Association of Firechiefs, Fairfax
Morphix Technologies, Inc., Virginia Beach
QinetiQ, Inc., Arlington
SET Associates, Arlington
Sparta, Inc., Arlington
Stratech Systems, Inc., McLean
System Planning Corporation, Arlington
The Institute for Applied Science, Reston
Titan Corporation, Reston
University of Virginia, Charlottesville
Vertex Solutions, Falls Church

### Washington
Advanced Interactive Systems, Inc., Seattle
Cascade Designs, Inc., Seattle
Isotron Corporation, Seattle
MesoSystems Technology, Inc., Kennewick
Pacific Northwest National Laboratory, Richland
Specialty Products, Inc., Lakewood

### West Virginia
MD BioTech, Morgantown
West Virginia High Technology Consortium Foundation, Fairmont
West Virginia University, Morgantown

### Wisconsin
Interspiro, Inc., Pleasant Prairie

### Wyoming
Aristatek, Inc., Laramie

## International

### Australia
QR Sciences, Ltd., Perth, Western Australia

### Canada
Argon Security Technologies, Inc., Port Moody, British Columbia
Bosik, Ottawa, Ontario
British Columbia Institute of Technology, Burnaby, British Columbia
Canadian Explosives Research Laboratory, Ottawa, Ontario
Defence Research and Development Canada, Suffield
Defence Research and Development Canada, Valcartier, Quebec
EOD Performance, Inc., Ottawa, Ontario
INFOSAT Telecommunication, Montreal, Quebec
Med-Eng Systems, Inc., Ottawa, Ontario

# 2005 Performers

Natural Resources Canada, Canadian Explosives Research Laboratory, Ottawa, Ontario
Royal Canadian Mounted Police, Ottawa, Ontario
Smiths Detection, Mississauga, Ontario
Vanguard Protective Technologies, Ltd., Ottawa, Ontario

### France
University of Rennes, Brittany

### Israel
Atlas Researches, Ltd., Hod Hasharon
Electro-Optics Industries, Ltd., Rehovat
Israel Institute for Biological Research, Ness-Ziona
Israel Police National HQ, Jerusalem
Ministry of Defense, Tel Aviv
National Information Security Agency, Tel Aviv
Rafael Armament Development Authority, Ltd., Haifa
Tadiran Communications Ltd., Holon

### United Kingdom
Defence Science and Technology Laboratories, Fort Halstead, Kent
Forensic Science Service, Birmingham, West Midlands
Forensic Science Service, London
Hazard Management Solutions, Ltd., Faringdon, Oxfordshire
Home Office Scientific Development Branch, Sandridge, Hertfordshire
QinetiQ, Ltd., Farnborough, Hampshire
QinetiQ, Ltd., Malvern, Worcestershire
The University of Sheffield, Department of Forensic Pathology, Sheffield, South Yorkshire

# Glossary of Acronyms

**A**

| | |
|---|---|
| ACC | Air Combat Command |
| ADL | Advanced Distributed Learning |
| AFESC | Air Force Electronic Systems Center |
| AFIP | Armed Forces Institute of Pathology |
| AFIS | Automated Fingerprint Identification System |
| AFRL | Air Force Research Lab |
| ANSI | American National Standards Institute |
| APBI | Advance Planning Briefing to Industry |
| APHIS | Animal and Plant Health Inspection Service |
| APV | Armored Passenger Vehicle |
| ARIS | Advanced Radioisotope Identification System |
| ARL | Army Research Laboratory |
| ARS | Agricultural Research Service |
| ASD(SO/LIC) | Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict |
| ASDE-3 | Airport Surface Detection Equipment |
| ATF | Bureau of Alcohol, Tobacco, Firearms, and Explosives |
| AVIDS | Advanced Vehicle/Driver Identification System |

**B**

| | |
|---|---|
| BAA | Broad Agency Announcement |
| BIDS | BAA Information Delivery System |
| BLIS | Blast Effects Information System |
| BUMED | Bureau of Medicine and Surgery |
| BX | Blast Effects and Mitigation |

**C**

| | |
|---|---|
| CB | Chemical and/or Biological |
| CBIRF | Chemical Biological Incident Response Force |
| CBRN | Chemical, Biological, Radiological, and Nuclear |
| CBRNC | Chemical, Biological, Radiological, and Nuclear Countermeasures |
| CDC | Centers for Disease Control and Prevention |
| CE | Corps of Engineers |
| CE-PDC | Corps of Engineers Protective Design Center |
| CENTCOM | Central Command |
| CID | Criminal Investigation Division (U.S. EPA) |
| CID | Criminal Investigation Command (U.S. Dept. of Defense) |
| CIRTS | Critical Incident Response Technology Seminars |
| CML Bn(TE) | Chemical Battalion (Technical Escort) |
| CMLS | Chemical School |
| COTS | Commercial-off-the-Shelf |
| CRADA | Cooperative Research and Development Agreement |
| CTTS | Combating Terrorism Technology Support |
| CTTSO | Combating Terrorism Technology Support Office |

# Glossary of Acronyms

**D**

| | |
|---|---|
| DARPA | Defense Advanced Research Projects Agency |
| DATSD (CBD) | Office of the Deputy Assistant to the Secretary of Defense for Chemical and Biological Defense |
| DCFL | Defense Computer Forensics Laboratory |
| DEA | Drug Enforcement Administration |
| DHS | Department of Homeland Security |
| DIA | Defense Intelligence Agency |
| DiCAST | Distributed Chemical Agent Sensing and Transmission |
| DLA | Defense Logistics Agency |
| DMNB | Dimethyl Dinitrobutane |
| DoD | Department of Defense |
| DoDPI | Department of Defense Polygraph Institute |
| DOE | Department of Energy |
| DOJ | Department of Justice |
| DOS | Department of State |
| DS | Bureau of Diplomatic Security |
| DTRA | Defense Threat Reduction Agency |

**E**

| | |
|---|---|
| ECBC | Edgewood Chemical Biological Center |
| ED | Explosives Detection |
| EMRTC | Energetic Materials Research and Testing Center |
| EOD | Explosive Ordnance Disposal |
| EOD Tech Det | Explosive Ordnance Disposal Technical Detachment |
| EPA | Environmental Protection Agency |
| EUCOM | European Command |

**F**

| | |
|---|---|
| FAA | Federal Aviation Administration |
| FAMS | Federal Air Marshal Service |
| FBI | Federal Bureau of Investigation |
| FBOP | Federal Bureau of Prisons |
| FDA | Food and Drug Administration |
| FDL | Forensic Document Laboratory |
| FEMA | Federal Emergency Management Agency |
| FPS | Federal Protective Service |
| FS | Forest Service |
| FSIS | Food Safety and Inspection Service |
| FY | Fiscal Year |

**G**

| | |
|---|---|
| GSA | General Services Administration |

**H**

| | |
|---|---|
| HQ | Headquarters |
| HRT | Hostage Rescue Team |
| HSARPA | Homeland Security Advanced Research Projects Agency |

# Glossary of Acronyms

**I**

| | |
|---|---|
| ICE | Immigration and Customs Enforcement |
| IDD | Improvised Device Defeat |
| IED | Improvised Explosive Device |
| IG/T | Interdepartmental Group on Terrorism |
| IGTA | International Group of Treasury Associations |
| IP | Infrastructure Protection |
| IPPS | Instantaneous Personnel Protection System |
| ISF | Investigative Support and Forensics |
| IWG/CT | Interagency Working Group on Counterterrorism |

**J**

| | |
|---|---|
| JCS | Joint Chiefs of Staff |
| JFCOM | Joint Forces Command |

**L**

| | |
|---|---|
| LDV | Laser Doppler Vibrometry |

**M**

| | |
|---|---|
| MANPADS | Man-Portable Air Defense Systems |
| MANSCEN | Maneuver Support Center |
| MCD | Marine Corps Detachment |
| MCNOSC | Marine Corps Network Operations and Security Command |
| MIT | Massachusetts Institute of Technology |
| MP School | Military Police School |

**N**

| | |
|---|---|
| NATO | North Atlantic Treaty Organization |
| NAVCENT | Naval Forces Central Command |
| NAVEODFLTLAU | Naval Explosive Ordnance Disposal Fleet Liaison Office |
| NAVEODTECHDIV | Naval Explosive Ordnance Disposal Technology |
| NAVFAC | Naval Facilities Engineering Command |
| NAVSEA | Naval Sea Systems Command |
| NAWC | Naval Air Warfare Center |
| NCFS | National Center for Forensic Science |
| NCIS | Naval Criminal Investigative Service |
| NEIC | National Enforcement Investigations Center |
| NFESC | Naval Facilities Engineering Service Center |
| NFPA | National Fire Protection Association |
| NFSTC | National Forensic Science Technology Center |
| NGIC | National Ground Intelligence Center |
| NHRC | Naval Health Research Center |
| NIJ | National Institute of Justice |
| NIOSH | National Institute for Occupational Safety and Health |
| NIST | National Institute of Standards and Technology |
| NNSA | National Nuclear Security Administration |
| NRL | Naval Research Laboratory |
| NSA | National Security Agency |
| NSWC | Naval Surface Warfare Center |

# Glossary of Acronyms

**O**

| | |
|---|---|
| OBO | Overseas Building Operations |
| OEA | Office of Energy Assurance |
| OLES | Office of Law Enforcement Standards |
| OSI | Office of Special Investigations |
| OSST | Open Source Security Tool Set |
| OUSD (P&R) | Office of the Under Secretary of Defense for Personnel and Readiness |

**P**

| | |
|---|---|
| PAN | Percussion Actuated Non-Electric |
| PAWS | Portable Armor Wall System |
| PDA | Personal Digital Assistant |
| PDC | Protective Design Center |
| PFPA | Pentagon Force Protection Agency |
| PKI | Public Key Infrastructure |
| PM-FPS | Product Manager for Force Protection Systems |
| PNNL | Pacific Northwest National Laboratory |
| PPE | Personal Protective Equipment |
| PS | Physical Security |
| PSG | Personnel Screening Guide |

**R**

| | |
|---|---|
| R&D | Research and Development |
| RAM | Random Access Memory |
| RCIED | Radio-Controlled Improvised Explosive Device |
| RCV | Remote Controlled Vehicle |
| RDECOM | Research, Development, and Engineering Command |
| RDX | Royal Demolition Explosive |
| RF | Radio Frequency |
| RFW | Radio-Frequency Weapon |
| RIG | Railcar Inspection Guide |
| RRA | Recoil Reduction Adapter |

**S**

| | |
|---|---|
| S/CT | Department of State Office of the Coordinator for Counterterrorism |
| S&T | Science and Technology |
| S-ACARS | Secure Aircraft Communications Addressing and Reporting System |
| SAFETY Act | Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 |
| SCADA | Supervisory Control and Data Acquisition |
| SCORM` | Shareable Content Object Reference Model |
| SCOS | Surveillance, Collection, and Operations Support |
| SO | Office of Security (U.S. Dept. of Energy) |
| SO/LIC | Special Operations and Low-Intensity Conflict |
| SOCOM | Special Operations Command |
| SPAWAR | Space and Naval Warfare Systems Command |
| SSC | Soldier Systems Center (Natick) |
| SSD | Special Services Division |
| SSD | Specialized Search Dog |
| SWAT | Special Weapons and Tactics |

# Glossary of Acronyms

**T**

| | |
|---|---|
| TACOM | Tank-Automotive and Armaments Command |
| TATP | Triacetone Triperoxide |
| TIC | Toxic Industrial Chemical |
| TOS | Tactical Operations Support |
| TOVA | Totally Optical Vapor Analyzer |
| TRADOC | Training and Doctrine Command |
| TSA | Transportation Security Administration |
| TSD | Technical Security Division |
| TSP | Training Support Package |
| TSWG | Technical Support Working Group |
| TTD | Training Technology Development |
| TTFD | Tactical Timed Firing Device |
| TVSS | Tactical Video Surveillance System |

**U**

| | |
|---|---|
| UCSD | University of California at San Diego |
| UNLV | University of Nevada at Las Vegas |
| USA | United States Army |
| USAF | United States Air Force |
| USAISR | United States Army Institute of Surgical Research |
| USAR | United States Army Reserve |
| USCG | United States Coast Guard |
| USMC | United States Marine Corps |
| USMS | United States Marshals Service |
| USN | United States Navy |
| USNAVEUR | United States Naval Forces Europe |
| USSS | United States Secret Service |

**V**

| | |
|---|---|
| VBIED | Vehicle-Borne Improvised Explosive Device |
| VIP | Very Important Person |
| VPAT | Virus Propagation Analysis Tool |
| VSP | Visual Sample Plan |


# Combating Terrorism Technology Support Office